3 1761 11648363 7

Digitized by the Internet Archive
in 2023 with funding from
University of Toronto

https://archive.org/details/31761116483637

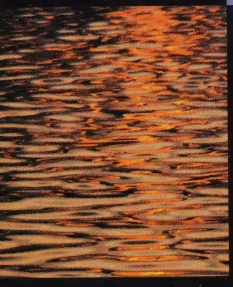
CA1 (118)
ND 800
-S16

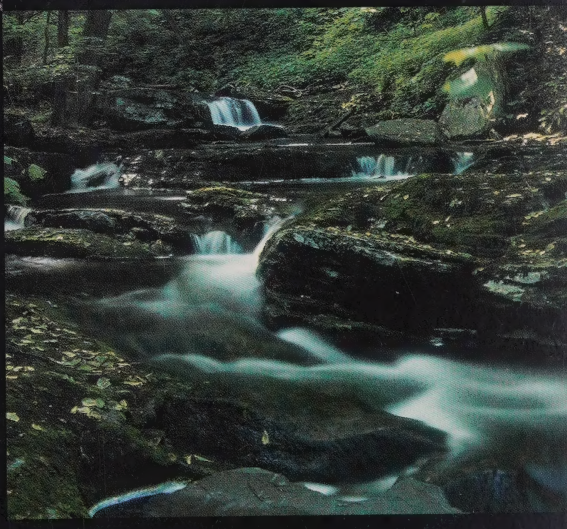
GOVT

COMMUNICATIONS
SECURITY
ESTABLISHMENT
COMMISSIONER

Annual Report







2010-2011

Canada

Office of the Communications Security
Establishment Commissioner
P.O. Box 1984, Station "B"
Ottawa, Ontario
K1P 5R5

Tel.: (613) 992-3044
Fax: (613) 992-4096
Website: www.ocsec-bccst.gc.ca

© Minister of Public Works and
Government Services Canada 2011
Cat. No. D-95-2011

Cover photos: Malak

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C103458

Communications Security
Establishment Commissioner

The Honourable Robert Décary, Q.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Robert Décary, c.r.

June 2011

LIBRARY
SEP 20 2011
University of Toronto

Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Sir:

Pursuant to subsection 273.63(3) of the *National Defence Act*, I am pleased to submit to you my annual report on my activities and findings for the period of April 1, 2010, to March 31, 2011, for your submission to Parliament.

Yours sincerely,

Robert Décary

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

TABLE OF CONTENTS

Commissioner's Message /1

Mandate of the Communications Security Establishment Canada /3

Mandate of the Communications Security Establishment Commissioner /5

Commissioner's Office /7

Overview of 2010–2011 Findings and Recommendations /11

Highlights of the Six Review Reports Submitted to the Minister in 2010–2011 /14

1. Review of CSEC information technology security activities conducted under ministerial authorization (Activity 1) /14

2. Review of CSEC information technology security activities conducted under ministerial authorization (Activity 2) /16

3. Combined annual review of CSEC foreign signals intelligence collection activities conducted under ministerial authorizations /18

4. Review of CSEC activities carried out under a ministerial directive and used by CSEC to identify new foreign entities believed to be of foreign intelligence interest /20

5. Review of the process by which CSEC determines that entities of foreign intelligence interest are foreign entities located outside of Canada, as required by the *National Defence Act* /23

6. Annual review of CSEC disclosures of information about Canadians to Government of Canada clients /25

Complaints About CSEC's Activities /27

Duty Under the *Security of Information Act* /27

Activities of the Commissioner's Office /28

Work Plan — Reviews Underway and Planned /30

The Upcoming Year /31

Annex A: Mandate of the CSEC — Excerpts from the *National Defense Act* /33

Annex B: Mandate of the Communications Security Establishment Commissioner — Excerpts from the *National Defense Act* and the *Security of Information Act* /35

Annex C: History of the Office of the Communications Security Establishment Commissioner /37

Annex D: Statement of Expenditures 2010–2011 /39

Annex E: Commissioner's Office Review Program — Logic Model /41

Annex F: Classified Reports to the Minister /43

Annex G: Legislative Safeguards for Private Communications and Measures to Protect Information About Canadians /47

COMMISSIONER'S MESSAGE

I was appointed Commissioner of the Communications Security Establishment on June 18, 2010. I knew very little about the challenge that awaited me. I knew that I was following in the footsteps of illustrious colleagues whom I had the privilege of knowing during my career (Chief Justices Bisson and Lamer, and Judges Gonthier and Cory). I knew that I would be involved in the highly technical and fascinating, albeit sensitive field, of security and the protection of the privacy of Canadians. As a lawyer and a Federal Court of Appeal judge, I had been involved in a number of privacy and terrorism cases. However, I would never have imagined the extent of the activities of the Communications Security Establishment Canada (CSEC), nor the critical and active role played by the Office of the Commissioner.

First, I wish to acknowledge the warm welcome that I received from the Office's team. I say "team" because they are a group of people who work together in a remarkable spirit of cooperation and strength of mind and of purpose. I especially appreciated the efforts that were made as soon as I arrived to explain to me in a clear and understandable manner the mandates and roles of the Office and of CSEC respectively. In this regard, I would also like to thank CSEC and its Chief, John Adams, who took considerable time and effort to convey the full nature and scope of CSEC's work. The information sessions that they organized for me were complex and intense, and I must say, well adapted to my needs.

During the first nine months of my mandate, I was impressed by the professionalism, objectivity, and rigour of my analysts. They know they have an important mission, especially in ensuring that the unintentional interception by CSEC of the private communications of Canadians is in compliance with the law. Consequently they leave no stone unturned in their reviews, which are conducted in an impressively detailed and comprehensive manner.

I was also impressed, and I must say surprised, because I was initially sceptical in this regard, with the degree of transparency and spirit of cooperation displayed by CSEC and its Chief. There have been, and will be, of course, significant differences of opinion between my office and CSEC on certain issues. However, overall, I can say that the protection of the privacy of Canadians is, in the eyes of CSEC and its employees, a genuine concern, which is more than I would have imagined at the beginning of my mandate.

During my appearance before the House of Commons' Standing Committee on National Defence on November 18, 2010, I stated in the following terms the dilemma faced by Parliament when passing the *Anti-Terrorism Act* in December 2001:

> Within Canada, every individual has a quasi-constitutional right with respect to his or her privacy. And every person has a constitutional right with respect to security of the person. In addition, the State has an obligation to protect each of these individual rights and to ensure the country's security as well. These rights and obligations are not easy to reconcile: what in fact would the right to privacy mean – or the right to security of the person – in a society where security was no longer taken for granted or that was no longer free and democratic?

I must reconcile these rights and obligations in the very specific context of the activities in which CSEC is engaged. It should be recalled that the first mandate of CSEC is to gather intelligence from foreign entities located outside Canada. CSEC is in fact prohibited by its governing legislation from "spying" on a Canadian wherever he or she might be in the world or on any individual in Canada. It is only unintentionally — and I would add unavoidable given the complexity, pervasiveness and interconnectedness of global telecommunications networks — that private communications are intercepted by CSEC. It is precisely because of this inevitability that the *National Defence Act* provides for ministerial authorization. The number of these intercepts, I hasten to emphasize, is very small.

During my first several months as Commissioner, I took the initiative to meet with the Minister of National Defence, the Chief of CSEC, the National Security Advisor to the Prime Minister, the Security Intelligence Review Committee, the Inspector General of the Canadian Security Intelligence Service, the Privacy Commissioner, and the interim Chair of the Commission for Public Complaints against the Royal Canadian Mounted Police. These meetings enabled me to gain a better appreciation not only of the scale of review activities in Canada but also of the opportunity for greater contact among the various review agencies.

Before explaining my role, I'd like to provide the reader with a clear understanding of CSEC's mandate.

MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

The *Anti-Terrorism Act* came into effect in December 2001, adding Part V.1 of the *National Defence Act*, and setting out CSEC's three-part mandate:

> Part (a) authorizes CSEC to collect foreign intelligence in accordance with the Government of Canada's intelligence priorities;
>
> Part (b) authorizes CSEC to help protect electronic information and information infrastructures of importance to the Government of Canada; and
>
> Part (c) authorizes CSEC to provide technical and operational help to federal law enforcement and security agencies, including obtaining and understanding communications collected under those agencies' own authorities.

The activities listed under parts (a) and (b) of CSEC's mandate are subject to three legislative limitations aimed at protecting Canadians' privacy:

1. CSEC is prohibited by law from directing its activities at Canadians – wherever they might be in the world – or at any person in Canada;

2. In conducting foreign intelligence or information technology security activities, CSEC may unintentionally intercept a one-end Canadian communication which is a private communication as defined by the *Criminal Code*. CSEC may use and retain this information only if it is essential to either international affairs, defence or security, or to identify, isolate or prevent harm to Government computer systems or networks; and

3. To provide a formal framework for the unintentional interception of private communications, the *National Defence Act* requires express authorization by the Minister of National Defence once he or she is satisfied that specific conditions provided for in the *National Defence Act* have been met. These are known as ministerial authorizations.

CSEC is prohibited from directing its activities at Canadians – wherever they might be in the world – or at any person in Canada.

In providing assistance under part (c) of its mandate, CSEC is subject to the same laws and limitations that govern the agencies it is assisting.

Annex A contains text of relevant sections of the *National Defence Act* relating to the role and mandate of CSEC. (p. 33)

MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

My mandate under the *National Defence Act* consists of three key functions:

1. **reviewing** CSEC activities to ensure they comply with the law;

2. **conducting** any investigations I deem necessary in response to complaints about CSEC; and

3. **informing** the Minister of National Defence and the Attorney General of Canada of any CSEC activities that I believe may not be in compliance with the law.

I also have a mandate under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy seeking to release special operational information on the grounds that it is in the public interest. To date, no such matters have been reported to a Commissioner.

Within the context of CSEC's mandate, the purpose of my reviews is:

- to ensure that activities conducted by CSEC under ministerial authorization are those authorized by the Minister of National Defence;
- to ensure that CSEC complies with the law and only directs its activities at foreign entities located outside Canada;
- to ensure that, in all the activities CSEC undertakes, it effectively applies satisfactory measures to protect the privacy of Canadians; and
- to report the results of my reviews to the Minister of National Defence, who is responsible for CSEC.

Additionally, each year I am required to submit a report to the Minister of National Defence on my activities, which the Minister must then table in Parliament.

My office is an autonomous agency with its own appropriation from Parliament.

While I am mandated to report to the Minister, my office is independent and separate from the Department of National Defence. My strong review mandate reflects the powers I have under the *Inquiries Act* as well as the independent nature of my office, which is an autonomous agency with its own appropriation from Parliament.

Annex B contains the text of the relevant sections of the *National Defence Act* and the *Security of Information Act* relating to my role and mandate as CSE Commissioner (p. 35) and **Annex C** describes the history of the Office of the CSE Commissioner. (p. 37)

COMMISSIONER'S OFFICE

I am supported in my work by a staff of eight, together with a number of subject-matter experts, under contract, as required. In 2010–2011, my office's expenditures were $1,605,422, which is within the allocated appropriation from Parliament.

Annex D provides the 2010-2011 Statement of Expenditures for the Office of the Communications Security Establishment Commissioner. (p. 39)

Objective of Review

The objective of my office's rigorous review process is to enable me to provide to the Minister of National Defence, and indeed to all Canadians, assurance that CSEC is complying with the law and protecting the privacy of Canadians. If I find an instance where CSEC has not complied with the law, I am obliged to inform the Minister of National Defence and the Attorney General of Canada.

Rigorous review enables me to provide the Minister assurance that CSEC is complying with the law.

Selection of activities for review

CSEC activities are selected for review and prioritized using a set of detailed criteria to help determine where risk is greatest for potential non-compliance with the law and for risks to privacy.

Selection and prioritization of subjects for review are documented in my three-year work plan, which is updated regularly as part of an ongoing process of assessing risk.

Risk is assessed by considering, among other factors:

- the controls placed on the activity to ensure compliance with legal, ministerial and policy requirements;
- whether the activity involves private communications or information about Canadians;
- whether the activity is new or how much time has passed since the last in-depth review of an activity;
- whether there have been significant changes to the authorities or technologies relating to the activity;
- whether Commissioners have made findings or recommendations relating to the activity which require follow-up; and
- issues arising in the public domain.

Review methodology and criteria

My staff test the contents of CSEC's databases.

In conducting a review, my staff examine CSEC's written and electronic records, including CSEC's policies and procedures and legal advice received from Justice Canada. My staff request briefings and demonstrations of specific activities, interview managers and employees and observe firsthand CSEC operators and analysts to verify how they conduct their work. My staff test information obtained against the contents of systems and databases. The work of CSEC's internal auditors and evaluators may also inform reviews.

Each review includes an assessment of CSEC's activities against a standard set of criteria, described below, consisting of legal requirements, ministerial requirements, and policies and procedures. Other criteria may be added, as appropriate.

Legal requirements: I expect CSEC to conduct its activities in accordance with the *National Defence Act*, the *Privacy Act*, the *Criminal Code*, the *Canadian Charter of Rights and Freedoms* and any other relevant legislation, and in accordance with Justice Canada advice.

Ministerial requirements: I expect CSEC to conduct its activities in accordance with ministerial direction, following all requirements and limitations set out in a ministerial authorization or directive.

Policies and procedures: I expect CSEC to have appropriate policies and procedures in place to guide its activities and to provide sufficient direction on legal and ministerial requirements and the protection of Canadians' privacy. I expect employees to be knowledgeable about and comply with policies and procedures. I also expect CSEC to employ an effective management control framework to ensure that the integrity and lawful compliance of its activities is maintained. This includes appropriate accounting for decisions taken and for information relating to compliance and the protection of the privacy of Canadians.

My review reports contain findings that confirm whether the above-noted criteria have been satisfactorily met by CSEC. These reports may also disclose the nature and significance of deviations from these criteria. In some cases, I make recommendations to the Minister which are aimed at correcting discrepancies between CSEC's activities and the expectations established by the review criteria. I monitor CSEC's efforts to address recommendations and respond to negative findings. As well, I monitor areas for follow-up identified in past reviews.

The Logic Model in **Annex E** provides a flow chart of our comprehensive review program. (p. 41)

Recommendations

Since 1997, my predecessors and I have submitted to the Minister of National Defence a total of 61 classified review reports and studies. In total, the reports contain 133 recommendations. CSEC has accepted and implemented or is working to address 95 percent (122 out of 129) of these recommendations. I am awaiting the Minister's response to the four recommendations I made in 2010-2011. This past year, CSEC completed work in response to three past recommendations and I am monitoring 18 recommendations that CSEC is working to address.

On occasion, CSEC may reject one of my recommendations. In this instance, I assess the reasons provided, in order to determine whether to accept them or to pursue the issue.

See **Annex F** for a complete list of the 61 classified review reports and studies submitted to the Minister of National Defence. (p. 43)

OVERVIEW OF 2010–2011 FINDINGS AND RECOMMENDATIONS

During the 2010–2011 reporting year, I submitted six reports to the Minister of National Defence on my review of CSEC activities.

These reviews were conducted under two areas of my mandate:

- ensuring CSEC activities are in compliance with the law — as set out in paragraph 273.63(2)(*a*) of the *National Defence Act*; and
- ensuring CSEC activities under a ministerial authorization are authorized — as set out in subsection 273.65(8) of the *National Defence Act*.

One review, which is now being done on an annual basis, related to disclosures of information about Canadians to Government of Canada departments and agencies. This review permits me to closely monitor CSEC activities involving Canadian identity information. Performing this review yearly allows me to verify that CSEC complies with the law and maintains measures to protect the privacy of Canadians.

Two reviews were conducted of CSEC information technology security activities conducted under ministerial authorizations.

Three reviews related to foreign signals intelligence activities, and included a review of how CSEC determines that entities of foreign intelligence interest are foreign entities located outside of Canada, as required by the *National Defence Act*.

The results

Overall, I am able to report that the activities of CSEC examined this year complied with the law.

My reviews in 2010-2011 also demonstrate that:

- CSEC takes seriously and acts on the Commissioner's recommendations. Over the past year CSEC addressed a number of deficiencies identified in previous reviews. My follow-up of these recommendations determined that CSEC addressed these deficiencies;

The activities of CSEC examined this year complied with the law.

- CSEC continued important work to incorporate information management practices into its core programs and has made it part of its employees' daily activities. This is important in enabling CSEC to demonstrate accountability for its activities and decisions; and

- CSEC has mature management, governance and internal oversight structures to guide and direct its operational activities.

In total this past year, I made four recommendations, two of which relate to reporting information to the Minister of National Defence with the objective of providing the Minister with a more complete picture of communications CSEC unintentionally intercepts and involving Canadians or persons in Canada. The other two recommendations strengthen policy guidance for certain foreign signals intelligence activities.

CSEC takes seriously and acts on the Commissioner's recommendations.

Past reviews of CSEC activities under ministerial authorizations have consistently demonstrated that the proportion of private communications that CSEC unintentionally intercepts is very small. Nevertheless, should there be an instance of non-compliance involving private communications, the potential impact on the privacy of Canadians could be significant, which is why I continue to focus my attention on this particular activity.

The proportion of private communications that CSEC unintentionally intercepts is very small.

See **Annex G** for information on legislative safeguards for private communications and information about Canadians. (p. 47)

HIGHLIGHTS OF THE SIX REVIEW REPORTS SUBMITTED TO THE MINISTER IN 2010-2011

1. Review of CSEC information technology security activities conducted under ministerial authorization (Activity 1)

Background

The *National Defence Act* mandates CSEC to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada.

This review examined certain information technology security activities conducted by CSEC under ministerial authorization in 2008–2009 at two Government of Canada departments. The activities examined help protect computer systems by detecting, analyzing, and mitigating sophisticated cyber attacks aimed at covertly accessing sensitive government computer networks.

My review followed-up on an operational issue that came to light in late 2006 and which had the potential for non-compliance. The Commissioner's 2007–2008 Annual Report commended the Chief of CSEC for his handling of this issue and for keeping the Commissioner informed of corrective steps.

The review also included an examination of CSEC's responses to the findings and recommendations of a previous review of information technology security activities at a specific Government of Canada department. These previous findings and recommendations related to ambiguities in policy, corporate record keeping and CSEC employees' awareness of their responsibilities for the activities. My review included examining a 2007 CSEC internal audit report relating to these activities.

Review rationale

Specific controls are placed on these information technology security activities to ensure they comply with legal, ministerial and policy requirements. Major changes to certain practices and to CSEC's policies and procedures relating to these activities recently occurred. This is the first review since CSEC restructured these activities. Past Commissioners have also made findings and recommendations on these activities.

Findings

- Based on information reviewed and interviews conducted, I found that CSEC's activities were authorized and carried out in accordance with the law, ministerial requirements, and CSEC's policies and procedures.
- CSEC's use and retention of unintentionally intercepted private communications and information about Canadians complied with the law and CSEC policies.
- I am pleased to note that, in 2008–2009, CSEC made significant changes to the policies and procedures and to the accountability framework for these activities. I found the new policies and procedures to be comprehensive, containing satisfactory measures to protect the privacy of Canadians.
- CSEC also introduced processes that strengthen employee understanding of the compliance framework, policies and procedures. CSEC monitored the conduct of the activities to verify compliance with legal, ministerial and policy requirements, and retained a complete record of these activities.
- I am confident that the significant changes made to these information technology security activities address the previous findings and recommendations made in the Commissioner's 2006 review.

- Finally, this review included a follow-up examination of a principal CSEC information technology security software tool and database. I confirmed an observation made last year in this office's study of CSEC's information technology security activities not conducted under ministerial authorization: that a software tool used by CSEC has adequate functionality to restrict access to information in the system, to meet security and confidentiality requirements, and to protect the privacy of Canadians.

Recommendations

I made no recommendations.

2. Review of CSEC information technology security activities conducted under ministerial authorization (Activity 2)

Background

This review examined other information technology security activities, conducted for two Government of Canada departments in 2007–2008 and 2008–2009, under ministerial authorizations pursuant to the *National Defence Act*.

The activities at the two departments involved CSEC efforts to penetrate the departments' computer systems (under controlled circumstances) to demonstrate potential vulnerabilities and to test the departments' reactions to such attacks.

My examination included changes to the scope of these activities and to the technology used by CSEC. I assessed these changes in terms of their potential impact on the risk to compliance with the law and on the risk to privacy.

Review rationale

Major changes to certain practices, technologies and CSEC policies and procedures relating to these activities have recently occurred. Specific controls are placed on these activities to ensure compliance with legal, ministerial and policy requirements, while protecting the privacy of Canadians. Past Commissioners had also made findings and recommendations concerning these activities. This is the first review since CSEC restructured these activities.

Findings

- Based on information reviewed and interviews conducted, I found that CSEC's activities were authorized and carried out in accordance with the law, ministerial requirements and CSEC policies and procedures.
- I found that the new policies and procedures were comprehensive and contained satisfactory measures to protect the privacy of Canadians.
- The record of the activities demonstrated that CSEC's new management control framework provides strong monitoring and compliance validation tools, which help ensure compliance with the law and the protection of Canadians' privacy.
- Changes to the technology and its application by CSEC did not impact on the risk to compliance with the law or on the risk to privacy.

Recommendations

I made no recommendations.

3. Combined annual review of CSEC foreign signals intelligence collection activities conducted under ministerial authorizations

Background

This was the first combined annual review of all foreign signals intelligence collection programs. I am required by the *National Defence Act* to review activities under ministerial authorization. The 2009–2010 Annual Report that I submitted to the Minister describes the recent introduction of the office's horizontal review approach, which involves a thorough examination of processes common to all CSEC foreign intelligence collection activities under ministerial authorization. For example, common to all collection methods are the processes by which CSEC: identifies, selects and directs its activities at entities of foreign intelligence interest; uses, shares, reports, retains or disposes of intercepted information; and takes measures to protect private communications and information about Canadians. My review included examining a CSEC internal audit report relating to these activities.

Review rationale

The horizontal review approach led to a re-assessment of how my office reviews ministerial authorizations. Given that common processes are examined in horizontal reviews, it was determined that this combined annual review of foreign signals intelligence ministerial authorizations would focus on any significant changes and on any private communications unintentionally intercepted by CSEC.

I looked for changes to the authorities and scope of the programs, to the technology used by CSEC, and to the associated management control frameworks. I assessed any changes in terms of their impact on the risk to compliance with the law and on the risk to privacy.

I examined certain metrics relating to interception and the privacy of Canadians. The purpose was to establish a baseline of key information, to examine trends and to allow identification of any significant changes over time. These metrics will also inform the risk assessment process and the development of my review work plan.

Another objective of this review was to examine a sample of private communications intercepted by CSEC under foreign intelligence ministerial authorizations but which had not been used in CSEC reporting. The purpose was to assess whether this sample contained foreign intelligence essential to international affairs, defence or security, as required by the *National Defence Act*.

Findings

The extent to which I assessed CSEC's compliance with the law was determined by this review's focus on identifying and understanding significant changes to the foreign signals intelligence collection programs.

- Within this context, and based on information reviewed and interviews conducted, I found that the activities were authorized under the *National Defence Act* and there was no indication of unlawful activity by CSEC. CSEC met ministerial requirements, and has effective policies and procedures in place to guide its activities.
- There are positive trends in policy development and in the clarity and consistency of the requests for ministerial authorizations. Within the overall amount of communications intercepted by CSEC, I found that the proportion of recognized private communications that had been unintentionally intercepted remained very small.

CSEC retained only those private communications essential to Canada's international affairs, defence, or security.

- Overall, the foreign signals intelligence collection programs did not change significantly, and as a result, I determined that it is not necessary at this time to conduct an in-depth review of any of these programs.
- With regard to the sample of private communications, based on the information reviewed and interviews conducted, I found that CSEC retained only those private communications essential to Canada's international affairs, defence, or security, as required by law.

Recommendations

I made three recommendations. Two of the recommendations dealt with reporting to the Minister of National Defence certain information relating to privacy, and including in the ministerial authorizations a requirement to report this information. This information is necessary to provide the Minister with a complete picture of CSEC's collection activities and to support the Minister in his accountability for CSEC, including for the measures CSEC takes to protect the privacy of Canadians.

I also recommended that, given the importance of ensuring legal compliance and the protection of Canadians' privacy, CSEC should accelerate the timeline for implementation of an improved policy for the active monitoring of activities under foreign signals intelligence ministerial authorizations.

As of the end of the 2010-2011 reporting period, March 31, 2011, I am awaiting the Minister's response to these recommendations and will note them in next year's annual report.

4. Review of CSEC activities carried out under a ministerial directive and used by CSEC to identify new foreign entities believed to be of foreign intelligence interest

Background

The *National Defence Act* mandates CSEC to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities.

CSEC conducts a number of activities for the purposes of locating new sources of foreign intelligence. When other means have been exhausted, CSEC may use information about Canadians when it has reasonable

grounds to believe that using this information may assist in identifying and obtaining foreign intelligence. CSEC conducts these activities infrequently, but they can be a valuable tool in meeting Government of Canada intelligence priorities. CSEC does not require a ministerial authorization to conduct these activities because they do not involve interception of private communications. However, a ministerial directive provides guidance on the conduct of these activities.

In recent years, three reviews have involved some degree of examination of these activities: a Review of CSEC's foreign intelligence collection in support of the Royal Canadian Mounted Police (RCMP) (Phase II) (2006); a Review of CSEC's activities carried out under a (different) ministerial directive (2008); and a Review of CSEC's support to the Canadian Security Intelligence Service (CSIS) (2008).

In his 2006–2007 Annual Report, the late Commissioner Gonthier questioned whether the foreign signals intelligence part of CSEC's mandate (part (a) of its mandate) was the appropriate authority in all instances for CSEC to provide support to the RCMP in the pursuit of its domestic criminal investigations. In his 2007–2008 Annual Report, Commissioner Gonthier stated that pending a re-examination of the legal issues raised, no assessment would be made of the lawfulness of CSEC's activities in support of the RCMP under the foreign signals intelligence part of CSEC's mandate. He also noted that CSEC's support to CSIS raised similar issues. Commissioner Gonthier emphasized that although he was in agreement with the advice that the Department of Justice had provided to CSEC, he questioned which part of CSEC's mandate — part (a) or part (c), the assistance part of CSEC's mandate — should be used as the proper authority for conducting the activities.

Subsequent to these reviews and statements in the annual reports, the Chief of CSEC suspended these activities. CSEC then made significant changes to related policies, procedures and practices.

Review rationale

These activities involve CSEC's use and analysis of information about Canadians for foreign intelligence purposes. Specific controls are placed on these activities to ensure compliance with legal, ministerial and policy requirements. Major changes to certain policies, procedures and practices have recently occurred. This was the first review of these activities since the Chief of CSEC allowed their resumption under new policies and procedures. There were also related issues, findings and recommendations highlighted by my predecessors that required follow-up.

Findings

- Based on information reviewed and interviews conducted, I found that CSEC's activities were authorized and carried out in accordance with the law, ministerial requirements and CSEC's policies and procedures.
- I found that the new policies and procedures were comprehensive and contained satisfactory measures to protect the privacy of Canadians.
- Because of the significant changes made by CSEC to these activities and the positive results of this review, I am of the view that CSEC has addressed the previous findings and recommendations.
- I assessed that the new processes put in place by CSEC were consistent with part (a) of its mandate. I had no questions similar to those raised in previous years as to whether such activities would be more appropriately authorized under part (c) of CSEC's mandate.
- CSEC's new policies, guidelines and forms address findings and recommendations made by past Commissioners. CSEC managers and officials were knowledgeable about and complied with policies and procedures. CSEC managers routinely and closely monitored these activities to ensure they complied with the governing authorities.

Recommendations

I made no recommendations. However, given that these activities involve CSEC's use and analysis of information about Canadians, and therefore have the potential to affect their privacy, I have directed my office to monitor these activities to ensure they continue to be conducted in accordance with the law, ministerial requirements and CSEC's policies and procedures.

5. Review of the process by which CSEC determines that entities of foreign intelligence interest are foreign entities located outside of Canada, as required by the *National Defence Act*

Background

CSEC must also be able to identify those one-end Canadian private communications it can lawfully intercept under a ministerial authorization on the basis that the acquisition of these communications is unintentional and the interception is directed at a foreign entity located outside Canada. This process must contain measures to protect the privacy of Canadians.

For the period of September 2008 to December 2010, I examined and tested the process and practices by which CSEC determines that entities of foreign intelligence interest are foreign entities located outside of Canada.

Review rationale

These activities are the foundation of CSEC's foreign signals intelligence collection programs. Specific controls are placed on these activities to ensure they meet the legal, ministerial and policy requirements which are crucial to protecting Canadians' privacy.

Past Commissioners made findings and recommendations on these activities, which required follow-up. In addition, major changes to certain technologies and policies and procedures relating to these activities have recently occurred and others are in progress. This is one of the first in-depth horizontal reviews of a CSEC process common to all foreign intelligence collection methods.

Findings

- Based on information reviewed and interviews conducted, I found that the process by which CSEC determines that entities of foreign intelligence interest are foreign entities located outside of Canada is in accordance with the law, ministerial requirements, and CSEC's policies and procedures.
- CSEC has sufficient policies and processes to satisfy the legal requirement not to direct foreign signals intelligence interception activities at a Canadian (anywhere) or at any person in Canada.
- CSEC employees who were interviewed and observed in their work were knowledgeable about relevant policies and procedures and were applying them in the conduct of the activities. CSEC managers routinely and closely monitor the activities to ensure they comply with governing authorities.

CSEC takes measures in the design of its systems to promote compliance with the law and the protection of Canadians' privacy.

- CSEC takes measures in the design of associated systems and databases to promote compliance with the law and the protection of Canadians' privacy. I found that recent enhancements to these systems and databases assist in ensuring compliance with the law, ministerial requirements and policy. Additional planned enhancements will further improve compliance.
- I did find, however, certain deficiencies in some of the associated management systems and databases. I am pleased to note that CSEC is taking measures to address these deficiencies. I will monitor CSEC's efforts in this regard.

Recommendations

CSEC's policies and procedures generally provide sufficient direction to CSEC employees in protecting Canadians' privacy while determining that entities of foreign intelligence interest are foreign entities located outside of Canada. However, policies and procedures applicable to a certain foreign signals intelligence collection program provide only limited direction on the process and practices for such activities. I therefore recommended that CSEC provide specific guidance for these activities.

As of the end of the reporting period, March 31, 2011, I am awaiting the Minister's response to this recommendation and will note it in next year's annual report.

6. Annual review of CSEC disclosures of information about Canadians to Government of Canada clients

Background

This review fulfills a commitment in the 2009–2010 Annual Report to conduct an annual review of a sample of disclosures of information about Canadians to Government of Canada departments and agencies. The purpose is to verify that CSEC complies with the law and maintains measures to protect the privacy of Canadians.

Information about Canadians may be included in CSEC's reports if it is essential to understanding foreign intelligence. However, any information that identifies a Canadian must be suppressed in reports disseminated to government departments and agencies — that is, replaced by a generic reference such as "a named Canadian".

See **Annex G** for more detailed information on legislative safeguards for private communications and measures to protect information about Canadians. (p. 47)

When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC must verify that the requesting government department or agency has both the authority and operational justification for obtaining such information. Only then may CSEC provide this information.

This review encompassed a sample of approximately 20 percent of requests received by CSEC for disclosure of suppressed information about Canadians contained in foreign intelligence reports, from April to September 2010. The sample included disclosures made to all of the Government of Canada departments and agencies that requested, and were provided with, information about Canadians.

My office examined the forms that CSEC used to document the departments' and agencies' authorities and justifications of their need for information about Canadians, as well as the associated foreign intelligence reports.

Review rationale

CSEC's disclosure activities involve the sharing of information about Canadians. Should there be an instance of non-compliance while CSEC conducts these activities, the potential impact on the privacy of Canadians could be significant.

In addition, I assessed CSEC's activities in response to two recommendations in a February 2010 review report of my predecessor relating to: (a) providing tools to support the tracking of clients' requests for, and any associated disclosures of, suppressed information about Canadians; and, (b) improving the consistency and accuracy of CSEC reports to the Minister of National Defence about these activities.

Findings

- Based on information reviewed and interviews conducted, I found that CSEC's disclosure of suppressed information about Canadians to Government of Canada clients was conducted in compliance with the law.

- Policies and procedures were in place to provide sufficient direction to CSEC employees on the protection of the privacy of Canadians.
- CSEC employees were knowledgeable about, and acted in accordance with, policies and procedures. CSEC managers monitored activities to ensure CSEC employees complied with governing authorities.
- I am satisfied that CSEC's practices and the planned implementation of a new system will address previous recommendations and permit CSEC to better track and produce accurate and consistent metrics on these activities.

Recommendations

I made no recommendations but will continue to conduct an annual review of these activities to verify that CSEC continues to comply with the law and maintains measures to protect the privacy of Canadians. I will also monitor CSEC efforts to implement the new system.

COMPLAINTS ABOUT CSEC'S ACTIVITIES

My mandate includes undertaking any investigation I deem necessary in response to a complaint — for example to determine whether CSEC has engaged, or is engaging, in unlawful activity or is not taking sufficient measures to protect the privacy of Canadians.

In 2010–2011, there were no complaints that warranted investigation.

DUTY UNDER THE *SECURITY OF INFORMATION ACT*

I have a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy seeking to defend the release of special operational information on the grounds that it is in the public interest. No such matters were reported in 2010–2011.

ACTIVITIES OF THE COMMISSIONER'S OFFICE

Appearance before the Standing Committee on National Defence

As I mentioned in my introduction, in November 2010 I appeared for the first time before the House of Commons Standing Committee on National Defence, which examined my nomination. I was thankful for the opportunity to meet with the Committee so early in my mandate, to describe my experiences, and to provide an overview of the legislative framework for CSEC and my role and activities. My remarks to the Committee are available on my office's website at www.ocsec-bccst.gc.ca. I look forward to other opportunities to appear before this or other committees of Parliament to discuss my activities and findings or to discuss the importance of review generally.

British Intelligence and Security Committee of Parliamentarians

I met with the British Intelligence and Security Committee of Parliamentarians during the Committee's visit to Ottawa in March 2011. Committee members and my officials and I exchanged information on challenges and best practices in review methodologies and compared differences in respective models for the review of security and intelligence agencies.

Review Agencies Forum

Since 2005, the Review Agencies Forum has brought together officials from my office, the Security and Intelligence Review Committee (SIRC), the Office of the Inspector General of the Canadian Security Intelligence Service, the Commission for Public Complaints against the Royal Canadian Mounted Police (CPC) and the Office of the Privacy Commissioner. The Forum met in January 2011 to discuss issues of common interest.

Training

During 2010, my office developed, and in November delivered, a review workshop for personnel of organizations dedicated to the review of law enforcement and security and intelligence agencies. This workshop contributed to training individuals in these review bodies. The purpose is to enhance the effectiveness of independent review. Another workshop will be held in the fall of 2011.

My office developed and delivered a review workshop.

Several of my staff received training from CSEC in the use of a specific CSEC foreign intelligence database. I would like to express appreciation to CSEC for this training.

Other activities

In October 2010, my office participated in the annual Canadian Association of Security and Intelligence Studies conference in Ottawa. The theme of the conference was Understanding National Security. Leading experts from Canada and abroad provided perspectives on issues of importance to the security and intelligence and review communities.

In December 2010, my office's Executive Director and I met with the Privacy Commissioner of Canada and the Assistant Privacy Commissioner to discuss our respective roles and responsibilities. The Executive Director also participated in a workshop and provided input into the development of an Office of the Privacy Commissioner reference guide for government policy makers.

In March 2011, my office's Executive Director, along with the former Chair of the CPC and the Executive Director of SIRC, participated in a training day for Justice Canada counsel working in the field of national security. The panel made presentations on the importance of review of law enforcement and security and intelligence agencies, including discussion of the findings and recommendations made in the inquiries led by the Honourable Justices O'Connor, Iacobucci and Major.

WORK PLAN — REVIEWS UNDERWAY AND PLANNED

The results of several reviews currently underway are expected to be reported on to the Minister of National Defence in the coming year and will be included in my 2011–2012 Annual Report.

The subjects of these reviews include: an annual review of occurrences identified by CSEC in 2010 that affected or had the potential to affect the privacy of a Canadian, and the measures taken by CSEC to address them; CSEC's foreign intelligence sharing with international partners; assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the *CSIS Act*; and CSEC's retention and disposal of intercepted information, and, in particular, of private communications and information about Canadians.

Other reviews planned for 2011–2012 include: CSEC information technology security activities conducted under Government of Canada departments' *Criminal Code* and *Financial Administration Act* authorities; activities conducted under CSEC information technology security ministerial authorizations; and particular activities of CSEC's operations centre. Some reviews may carry over into 2012–2013.

In addition, I will continue the annual reviews of foreign intelligence ministerial authorizations, of CSEC disclosures of information about Canadians to government clients, and of occurrences identified by CSEC that affected or had the potential to affect the privacy of a Canadian and the measures taken by CSEC to address them.

In addition to briefings on activities that we plan to review, the Commissioner's office requests briefings from CSEC to assist in determining risk and work plan development. We receive regular briefs on changes to the management and administration of CSEC operational-related programs, including changes to policies and procedures.

THE UPCOMING YEAR

I am beginning the second year of my mandate with optimism and realism. On the one hand, I am optimistic because of the quality of the team that assists me, the rigour of the review process established by the office, and the professionalism underlying relations between CSEC and my office. On the other hand, I am realistic given the constantly changing technological environment and an equally dynamic international environment, to which I and my team, as well as CSEC, must adapt. In this context, I want to ensure that CSEC maintains and reinforces the measures taken to protect the privacy of Canadians.

Our free and democratic society will always be subject to internal and external threats. Each technological development, for example, may have both positive and negative effects. The need to reconcile the right of everyone to a free and democratic society and the right of each person to the protection of his or her privacy demands rigorous and ongoing efforts on the part of those who, like us, have a mandate to ensure that the activities of agencies which operate in the greatest secrecy comply with the law and protect the privacy of Canadians.

The need to reconcile the right of everyone to a free and democratic society and the right of each person to the protection of his or her privacy demands rigorous and ongoing efforts.

My office will carry out several reviews during the upcoming year. I plan to pay special attention to those activities of CSEC which concern me the most and where the risks to privacy are the greatest. I want to ensure that CSEC does not use or retain any private communications that are not related to international affairs, defence, or security, which is a legal requirement. I also want to ensure that the identity of a Canadian is revealed only when it is strictly necessary. The risk to individual privacy is heightened when information is shared, particularly with international partners, and I will report next year on the review under way on this issue.

The part of CSEC's mandate dealing with the protection of information and the information infrastructures of importance to the Government of Canada has gained in prominence; recent incidents have reminded us to what degree our computer systems may be vulnerable. In this context, I have requested my officials to examine in-depth these CSEC activities of growing prominence to ensure that they comply with the law and protect the privacy of Canadians.

A final word on an issue that persists year after year: the need for legislative amendments that will eliminate the ambiguities noted by my predecessors and myself in the *National Defence Act*. I know that the work is under way. It is my hope that the new government elected on May 2nd 2011 will act quickly and that all Members of Parliament will support the elimination of these ambiguities. These legislative amendments, in my opinion, should not provoke any controversy.

ANNEX A: MANDATE OF THE CSEC — EXCERPTS FROM THE *NATIONAL DEFENSE ACT*

The Communications Security Establishment Canada (CSEC) is the national cryptologic agency, providing the Government of Canada with two key services: foreign signals intelligence, and information technology security. CSEC also provides technical and operational assistance to federal law enforcement and security agencies.

CSEC's foreign intelligence products and services support government decision-making in the fields of national security, national defence and foreign policy. CSEC's signals intelligence activities relate exclusively to foreign intelligence and are directed by the Government of Canada's intelligence priorities.

CSEC's information technology security products and services enable government departments and agencies to secure their electronic information systems and networks. CSEC also conducts research and development on behalf of the Government of Canada in fields related to communications security.

CSEC's three-part mandate is set out in subsection 273.64(1) of the *National Defence Act*:

(*a*) to aquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;

(*b*) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and

(*c*) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

CSEC's website is: www.cse-cst.gc.ca.

ANNEX B: MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER — EXCERPTS FROM THE *NATIONAL DEFENSE ACT* AND THE *SECURITY OF INFORMATION ACT*

***National Defence Act* – Part V.1**

273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

(2) The duties of the Commissioner are:

(*a*) to review the activities of the Establishment to ensure that they are in compliance with the law;

(*b*) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(*c*) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

[...]

273.65 (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

Security of Information Act

15. (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]

(5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]

(*b*) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

ANNEX C: HISTORY OF THE OFFICE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

The Office of the Communications Security Establishment Commissioner was created on June 19, 1996, with the appointment of the inaugural Commissioner, the Honourable Claude Bisson, O.C., a former Chief Justice of Québec, who held the position until June 2003. He was succeeded by the late Right Honourable Antonio Lamer, P.C., C.C., C.D., LL.D., D.U., former Chief Justice of Canada, for a term of three years. The Honourable Charles D. Gonthier, C.C., Q.C., who retired as Justice of the Supreme Court of Canada in 2003, was appointed as Commissioner in August 2006, a position he held until his death in July 2009. The Honourable Peter deC. Cory, C.C., C.D., a former Justice of the Supreme Court of Canada, served as Commissioner from December 14, 2009 to March 31, 2010. On June 18, 2010, the Honourable Robert Décary, Q.C., a former Justice of the Federal Court of Appeal, was appointed Commissioner.

For the first six years (from June 1996 to December 2001), the Commissioner carried out his duties under the authority of Orders in Council issued pursuant to Part II of the *Inquiries Act.* During this period, the Commissioner's responsibilities were twofold: to review the activities of the Communications Security Establishment Canada (CSEC) to determine whether they conformed with the laws of Canada; and to receive complaints about CSEC's activities.

The omnibus *Anti-terrorism Act,* which came into force on December 24, 2001, introduced amendments to the *National Defence Act* by adding Part V.1 and creating legislative frameworks for both the Commissioner's office and CSEC. It gave the Commissioner new responsibilities to review activities carried out by CSEC under a ministerial authorization. The legislation also continued the Commissioner's powers under the *Inquiries Act*.

The omnibus legislation also introduced the *Security of Information Act*, which replaced the *Official Secrets Act.* This legislation gives the Commissioner specific duties in the event that a person, who would otherwise be permanently bound to secrecy, seeks to defend the release of classified information about CSEC on the grounds that it is in the public interest.

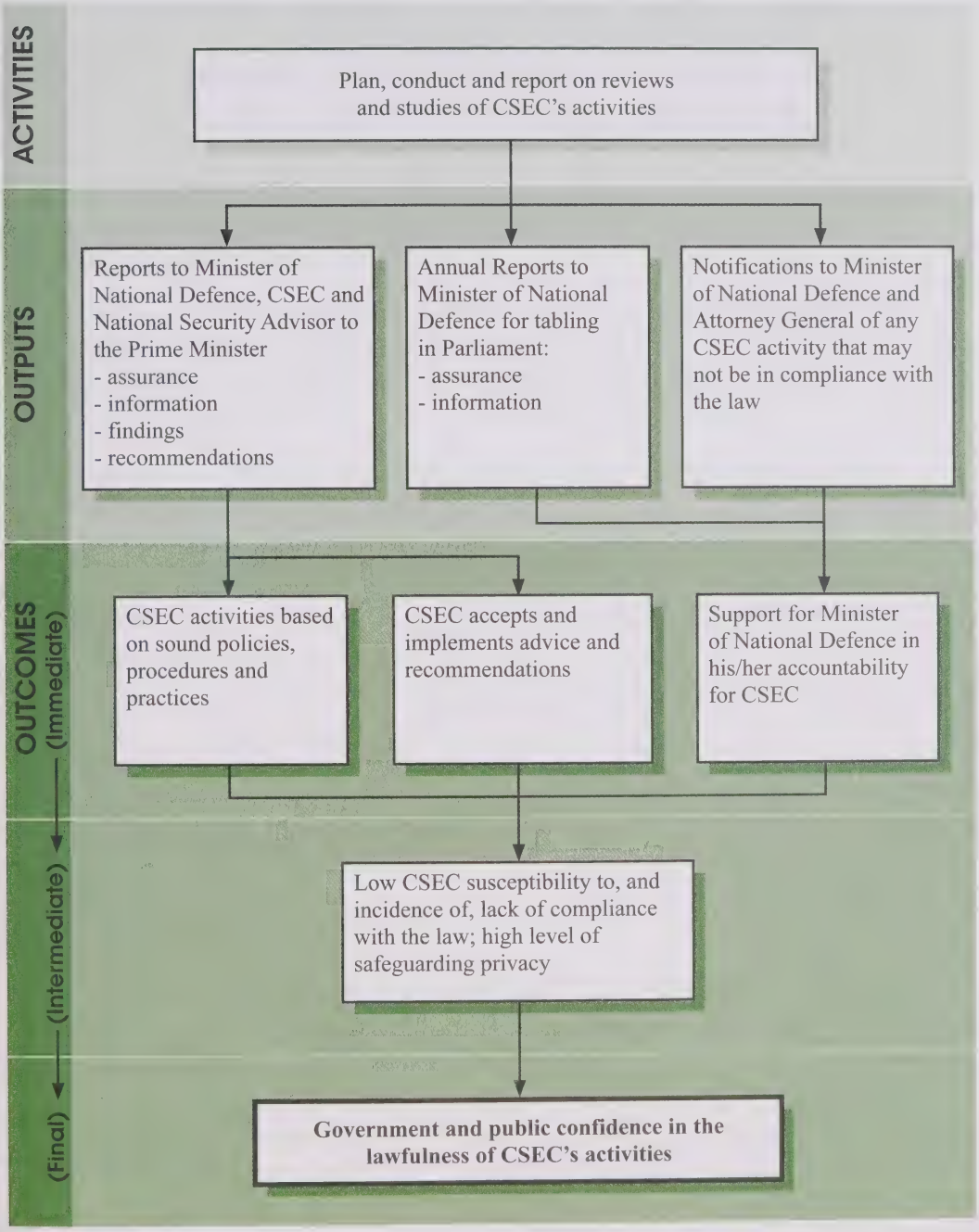
On April 1, 2009, the Commissioner's office was granted its own parliamentary appropriation. While the Commissioner continues to provide the Minister of National Defence with his reports, the Commissioner's office is separate from, and not part of, the Department of National Defence.

ANNEX D: STATEMENT OF EXPENDITURES 2010–2011

Standard Object Summary

Salaries and Wages	$ 890,939
Transportation and Telecommunications	12,995
Information	21,125
Professional and Special Services	457,655
Rentals	170,707
Purchased Repairs and Maintenance	1,249
Material and Supplies	33,252
Machinery and Equipment	17,500
Total	**$ 1,605,422**

ANNEX E: COMMISSIONER'S OFFICE REVIEW PROGRAM — LOGIC MODEL



ANNEX F: CLASSIFIED REPORTS TO THE MINISTER

1. Principal vs. agent status – March 3, 1997 (TOP SECRET)
2. Operational policies with lawfulness implications – February 6, 1998 (SECRET)
3. CSE's activities under *** – March 5, 1998 (TOP SECRET Codeword/CEO)
4. Internal investigations and complaints – March 10, 1998 (SECRET)
5. CSE's activities under *** – December 10, 1998 (TOP SECRET/CEO)
6. On controlling communications security (COMSEC) material – May 6, 1999 (TOP SECRET)
7. How we test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) – June 14, 1999 (TOP SECRET Codeword/CEO)
8. A study of the *** collection program – November 19, 1999 (TOP SECRET Codeword/CEO)
9. On *** – December 8, 1999 (TOP SECRET/COMINT)
10. A study of CSE's *** reporting process — an overview (Phase I) – December 8, 1999 (SECRET/CEO)
11. A study of selection and *** — an overview – May 10, 2000 (TOP SECRET/CEO)
12. CSE's operational support activities under *** — follow-up – May 10, 2000 (TOP SECRET/CEO)
13. Internal investigations and complaints — follow-up – May 10, 2000 (SECRET)
14. On findings of an external review of CSE's ITS program – June 15, 2000 (SECRET)
15. CSE's policy system review – September 13, 2000 (TOP SECRET/CEO)
16. A study of the *** reporting process — *** (Phase II) – April 6, 2001 (SECRET/CEO)
17. A study of the *** reporting process — *** (Phase III) – April 6, 2001 (SECRET/CEO)

18. CSE's participation *** – August 20, 2001 (TOP SECRET/CEO)

19. CSE's support to ***, as authorized by *** and code-named *** – August 20, 2001 (TOP SECRET/CEO)

20. A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – August 21, 2002 (SECRET)

21. CSE's support to ***, as authorized by *** and code-named *** – November 13, 2002 (TOP SECRET/CEO)

22. CSE's *** activities carried out under the *** 2002 *** Ministerial authorization – November 27, 2002 (TOP SECRET/CEO)

23. Lexicon of CSE definitions – March 26, 2003 (TOP SECRET)

24. CSE's activities pursuant to *** Ministerial authorizations including *** – May 20, 2003 (SECRET)

25. CSE's support to ***, as authorized by *** and code-named *** — Part I – November 6, 2003 (TOP SECRET/COMINT/CEO)

26. CSE's support to ***, as authorized by *** and code-named *** — Part II – March 15, 2004 (TOP SECRET/COMINT/CEO)

27. A review of CSE's activities conducted under *** Ministerial authorization – March 19, 2004 (SECRET/CEO)

28. Internal investigations and complaints — follow-up – March 25, 2004 (TOP SECRET/CEO)

29. A review of CSE's activities conducted under 2002 *** Ministerial authorization – April 19, 2004 (SECRET/CEO)

30. Review of CSE *** operations under Ministerial authorization – June 1, 2004 (TOP SECRET/COMINT)

31. CSE's support to *** – January 7, 2005 (TOP SECRET/COMINT/CEO)

32. External review of CSE's *** activities conducted under Ministerial authorization – February 28, 2005 (TOP SECRET/COMINT/CEO)

33. A study of the *** collection program – March 15, 2005 (TOP SECRET/COMINT/CEO)

34. Report on the activities of CSE's *** – June 22, 2005 (TOP SECRET)

35. Interim report on CSE's *** operations conducted under Ministerial authorization – March 2, 2006 (TOP SECRET/COMINT)

36. External review of CSE *** activities conducted under Ministerial authorization – March 29, 2006 (TOP SECRET/CEO)

37. Review of CSE's foreign intelligence collection in support of the RCMP (Phase II) – June 16, 2006 (TOP SECRET/COMINT/CEO)

38. Review of information technology security activities at a government department under ministerial authorization – December 18, 2006 (TOP SECRET)

39. Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – February 20, 2007 (TOP SECRET/COMINT/CEO)

40. Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – March 31, 2007 (TOP SECRET/COMINT/CEO)

41. Review of information technology security activities at a government department under ministerial authorization – July 20, 2007 (TOP SECRET)

42. Review of CSEC's counter-terrorism activities – October 16, 2007 (TOP SECRET/COMINT/CEO)

43. Review of CSEC's activities carried out under a ministerial directive – January 9, 2008 (TOP SECRET/COMINT/CEO)

44. Review of CSEC's support to CSIS – January 16, 2008 (TOP SECRET/COMINT/ CEO)

45. Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) – March 28, 2008 (TOP SECRET/COMINT/CEO)

46. Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians – June 11, 2008 (TOP SECRET/COMINT/CEO)

47. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1) – June 11, 2008 (TOP SECRET/COMINT/CEO)

48. Review of disclosure of information about Canadians to Government of Canada clients – November 19, 2008 (TOP SECRET/COMINT/CEO)

49. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2) – January 13, 2009 (TOP SECRET/COMINT/CEO)

50. Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3) – February 26, 2009 (TOP SECRET/COMINT/CEO)

51. Review of CSEC activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate – March 12, 2009 (TOP SECRET/COMINT Codeword/CEO)

52. Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive – March 12, 2009 (TOP SECRET/COMINT/CEO)

53. Study of CSEC information technology security activities not conducted under ministerial authorization – June 11, 2009 (TOP SECRET/COMINT/CEO)

54. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations and in support of government efforts relating to Afghanistan – January 18, 2010 (TOP SECRET/COMINT/CEO)

55. Regular review of CSEC disclosure of information about Canadians to Government of Canada clients – February 16, 2010 (TOP SECRET/COMINT/CEO)

56. Review of CSEC information technology security activities conducted under ministerial authorization (Activity 1) – October 18, 2010 (TOP SECRET/COMINT/CEO)

57. Review of CSEC activities carried out under a ministerial directive and used by CSEC to identify new foreign entities believed to be of foreign intelligence interest – December 16, 2010 (TOP SECRET/COMINT/CEO)

58. Review of CSEC information technology security activities conducted under ministerial authorization (Activity 2) – February 14, 2011 (SECRET)

59. Annual review of CSEC disclosures of information about Canadians to Government of Canada clients – February 21, 2011 (CONFIDENTIAL)

60. Combined annual review of CSEC foreign signals intelligence collection activities conducted under ministerial authorizations – February 25, 2011 (TOP SECRET/COMINT/CEO)

61. Review of the process by which CSEC determines that entities of foreign intelligence interest are foreign entities located outside of Canada, as required by the *National Defence Act* – March 15, 2011 (TOP SECRET/COMINT/CEO)

ANNEX G: LEGISLATIVE SAFEGUARDS FOR PRIVATE COMMUNICATIONS AND MEASURES TO PROTECT INFORMATION ABOUT CANADIANS

In the execution of its foreign intelligence and information technology security mandates, CSEC is expressly prohibited pursuant to paragraph 273.64(2)(*a*) of the *National Defence Act* from directing its activities at Canadian citizens, permanent residents or corporations, regardless of their location. CSEC is also prohibited from directing its activities at any person in Canada, regardless of their nationality.

However, due to the manner in which communications are transmitted, CSEC may, while conducting its mandated foreign signals intelligence or information technology security activities, unintentionally intercept communications of Canadians or persons in Canada, which constitute "private communications" under section 183 of the *Criminal Code*.

Recognizing this possibility, the *National Defence Act* allows the Minister of National Defence to authorize CSEC to intercept private communications. Prior to granting this authorization, however, the Minister must be satisfied that certain conditions set out in the *National Defence Act* are met. There are four conditions for foreign signals intelligence ministerial authorizations (subsection 273.65(2)) and five conditions for information technology security ministerial authorizations (subsection 273.65(4)).

CSEC's foreign signals intelligence and information technology security reports may contain information about Canadians (as defined in section 273.61 of the *National Defence Act*) if such information is deemed essential to the understanding of the reports. However, this information must be suppressed, that is replaced by a generic reference such as "a named Canadian" person or company. When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC must verify that the requesting government department or agency has both the authority and operational justification for obtaining such information. Only then may CSEC provide this information.

The provision of assistance to federal law enforcement and security agencies under paragraph 273.64(1)(*c*) of the *National Defence Act* is not subject to the statutory prohibition contained in paragraph 273.64(2)(*a*) of the *National Defence Act* against directing activities at Canadians located anywhere or at persons located in Canada, provided that the assisted agency has the lawful authority. CSEC is also subject pursuant to subsection 273.64(3) of the *National Defence Act* to any limitations imposed by law on the assisted agency in the performance of its duties.

L'aide accordée aux organismes fédéraux voués à l'application de la loi ou aux agences de sécurité en vertu de l'alinéa 273.64(1)*c*) de la *Loi sur la défense nationale* échappe à l'interdiction stipulée à l'alinéa 273.64(2)*a*) de la *Loi sur la défense nationale* selon laquelle les activités du CSTC ne doivent pas cibler des Canadiens, quel que soit l'endroit où ils se trouvent, ni des personnes au Canada, pourvu que l'organisme qui bénéficie de l'aide dispose d'une autorisation légale. Le CSTC est également tenu, en vertu du paragraphe 273.64(3) de la *Loi sur la défense nationale*, de respecter les limites imposées par la loi à l'organisme qu'il aide dans l'exécution de ses fonctions.

ANNEXE G : PROTECTION LÉGISLATIVE VISANT LES COMMUNICATIONS PRIVÉES ET MESURES DE PROTECTION DE L'INFORMATION CONCERNANT DES CANADIENS

Dans l'exécution de son double mandat de communication de renseignements étrangers et de sécurité des technologies de l'information, le CSTC se voit expressément interdire, en vertu de l'alinéa 273.64(2)*a*) de la *Loi sur la défense nationale*, de viser par ses activités des citoyens canadiens, des résidents permanents ou des sociétés canadiennes, peu importe le lieu où ils se trouvent. Le CSTC se voit également interdire d'exercer des activités visant une personne au Canada, peu importe sa nationalité.

Toutefois, en raison de la manière dont les communications sont transmises, le CSTC peut, tout en s'acquittant de la collecte de renseignements étrangers ou en menant ses activités relatives à la sécurité des technologies de l'information, intercepter de manière fortuite des communications de Canadiens ou de personnes au Canada, qui sont des « communications privées » au sens de l'article 183 du *Code criminel*.

Prenant en compte cette possibilité, la *Loi sur la défense nationale* permet au ministre de la Défense nationale d'autoriser le CSTC à intercepter des communications privées. Toutefois, avant d'accorder cette autorisation, le ministre doit être convaincu que certaines conditions établies dans la *Loi sur la défense nationale* sont remplies. Quatre conditions sont stipulées concernant les autorisations ministérielles de collecte de renseignements électromagnétiques étrangers (paragraphe 273.65 (2)) et cinq conditions visent les autorisations ministérielles relatives à la sécurité des technologies de l'information (paragraphe 273.65 (4)).

Les rapports du CSTC sur les renseignements étrangers et sur la sécurité des technologies de l'information peuvent renfermer de l'information concernant des Canadiens (au sens de l'article 273.61 de la *Loi sur la défense nationale*) si cette information est jugée essentielle à la compréhension du rapport. Toutefois, l'information doit être supprimée, c'est-à-dire remplacée par une mention spéciale du type « un Canadien » ou « une personne morale canadienne ». Lorsqu'il reçoit une demande subséquente de divulgation de précisions concernant l'information supprimée, le CSTC doit vérifier que le ministère ou organisme gouvernemental dont elle émane dispose à la fois de l'autorisation et d'une justification opérationnelle pour obtenir ce genre de renseignements. Ce n'est qu'après cette vérification que le CSTC peut fournir l'information.

51. Review of CSEC Activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate – 12 mars 2009 (TRÈS SECRET/ COMINT/Réservé aux Canadiens)

52. Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive – 12 mars 2009 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

53. Study of CSEC information technology security activities not conducted under ministerial authorization – 11 juin 2009 (TRÈS SECRET /COMINT/Réservé aux Canadiens)

54. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations and in support of government efforts relating to Afghanistan – 18 janvier 2010 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

55. Regular review of CSEC disclosure of information about Canadians to Government of Canada clients – 16 février 2010 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

56. Review of CSTC information technology security activities conducted under ministerial authorization (Activity 1) – 18 octobre 2010 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

57. Review of CSTC activities carried out under a ministerial directive and used by CSTC to identify new foreign entities believed to be of foreign intelligence interest – 16 décembre 2010 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

58. Review of CSTC information technology security activities conducted under ministerial authorization (Activity 2) – 14 février 2011 (SECRET)

59. Annual review of CSTC disclosures of information about Canadians to Government of Canada clients – 21 février 2011 (CONFIDENTIEL)

60. Combined annual review of CSTC foreign signals intelligence collection activities conducted under ministerial authorizations – 25 février 2011 (TRÈS SECRET/ COMINT/Réservé aux Canadiens)

61. Review of the process by which CSTC determines that entities of foreign intelligence interest are foreign entities located outside of Canada, as required by the *National Defence Act* – 15 mars 2011 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

37. Review of CSE'S foreign intelligence collection in support of the RCMP (Phase II) – 16 juin 2006 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

38. Review of information technology security activities at a government department under ministerial authorization – 18 décembre 2006 (TRÈS SECRET)

39. Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – 20 février 2007 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

40. Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – 31 mars 2007 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

41. Review of information technology security activities at a government department under ministerial authorization – 20 juillet 2007 (TRÈS SECRET)

42. Review of CSEC's counter-terrorism activities – 16 octobre 2007 (TRÈS SECRET/ COMINT/Réservé aux Canadiens)

43. Review of CSE's activities carried out under a ministerial directive – 9 janvier 2008 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

44. Review of CSEC's support to CSIS – 16 janvier 2008 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

45. Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) – 28 mars 2008 (TRÈS SECRET/OMINT/Réservé aux Canadiens)

46. Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians – 11 juin 2008 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

47. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1) – 11 juin 2008 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

48. Review of disclosure of information about Canadians to Government of Canada clients – 19 novembre 2008 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

49. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2) – 13 janvier 2009 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

50. Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3) – 26 février 2009 (TRÈS SECRET/ COMINT/Réservé aux Canadiens)

19. CSE's support to ***, as authorized by *** and code-named *** – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

20. A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – 21 août 2002 (SECRET)

21. CSE's support to ***, as authorized by *** and code-named *** – 13 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

22. CSE's *** activities carried out under the *** 2002 *** Ministerial authorization – 27 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

23. Lexicon of CSE definitions – 26 mars 2003 (TRÈS SECRET)

24. CSE's activities pursuant to *** Ministerial authorizations including *** – 20 mai 2003 (SECRET)

25. CSE's support to ***, as authorized by *** and code-named *** — Part I – 6 novembre 2003 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

26. CSE's support to ***, as authorized by *** and code-named *** — Part II – 15 mars 2004 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

27. A review of CSE's activities conducted under *** Ministerial authorization – 19 mars 2004 (SECRET/Réservé aux Canadiens)

28. Internal investigations and complaints — follow-up – 25 mars 2004 (TRÈS SECRET/ Réservé aux Canadiens)

29. A review of CSE's activities conducted under 2002 *** Ministerial authorization – 19 avril 2004 (SECRET/Réservé aux Canadiens)

30. Review of CSE *** operations under Ministerial authorization – 1er juin 2004 (TRÈS SECRET/COMINT)

31. CSE's support to *** – 7 janvier 2005 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

32. External review of CSE's *** activities conducted under Ministerial authorization – 28 février 2005 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

33. A study of the *** collection program – 15 mars 2005 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

34. Report on the activities of CSE's *** – 22 juin 2005 (TRÈS SECRET)

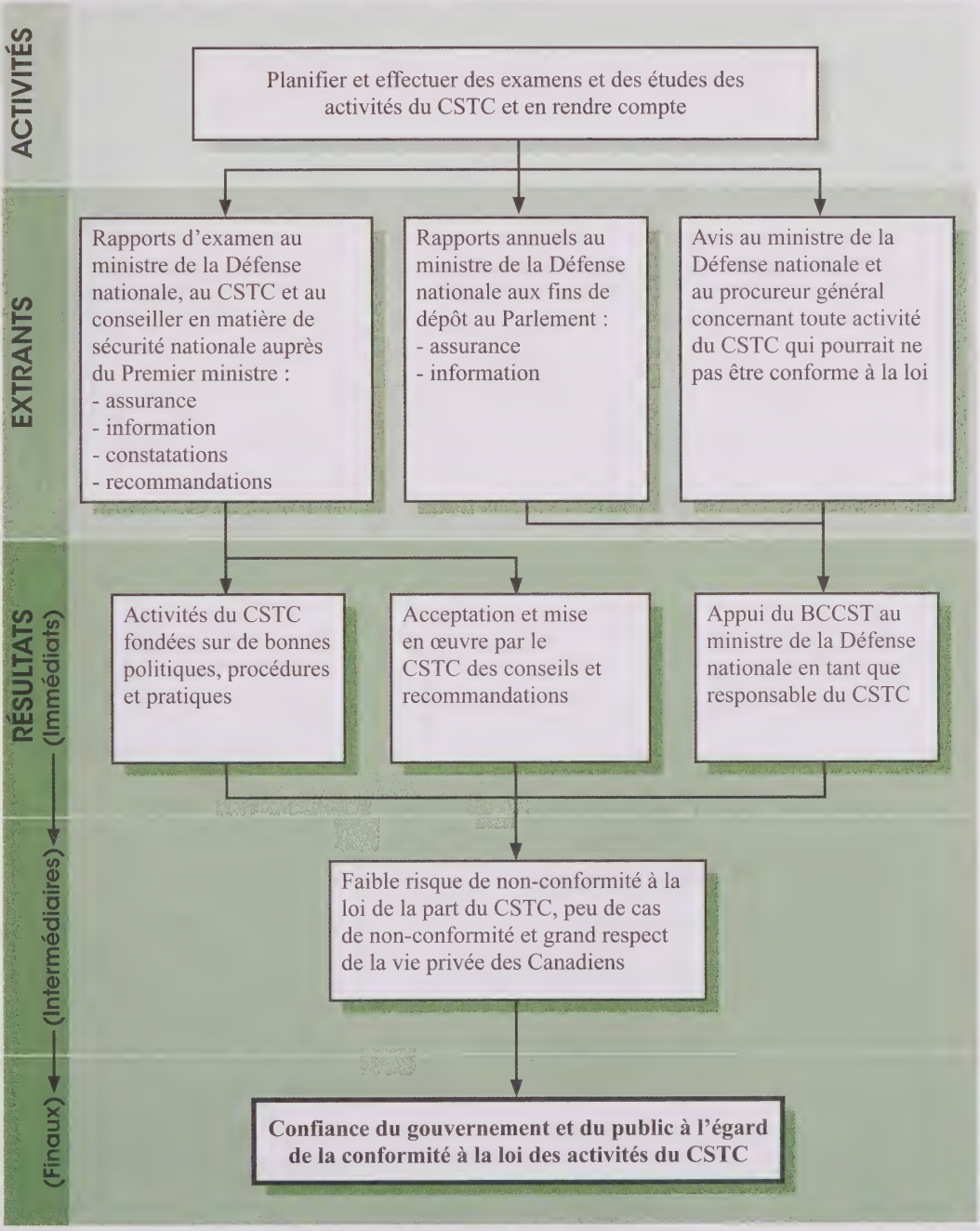
35. Interim report on CSE's *** operations conducted under Ministerial authorization – 2 mars 2006 (TRÈS SECRET/COMINT)

36. External review of CSE *** activities conducted under Ministerial authorization – 29 mars 2006 (TRÈS SECRET/Réservé aux Canadiens)

ANNEXE F : RAPPORTS CLASSIFIÉS SOUMIS AU MINISTRE

1. Principal vs. agent status – 3 mars 1997 (TRÈS SECRET)
2. Operational policies with lawfulness implications – 6 février 1998 (SECRET)
3. CSE's activities under *** – 5 mars 1998 (TRÈS SECRET Mot codé/ Réservé aux Canadiens)
4. Internal investigations and complaints – 10 mars 1998 (SECRET)
5. CSE's activities under *** – 10 décembre 1998 (TRÈS SECRET/Réservé aux Canadiens)
6. On controlling communications security (COMSEC) material – 6 mai 1999 (TRÈS SECRET)
7. How we test (Rapport classifié sur la mise à l'essai des pratiques du CSTC en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) – 14 juin 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)
8. A study of the *** collection program – 19 novembre 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)
9. On *** – 8 décembre 1999 (TRÈS SECRET/COMINT)
10. A study of CSE's *** reporting process — an overview (Phase I) – 8 décembre 1999 (SECRET/Réservé aux Canadiens)
11. A study of selection and *** — an overview – 10 mai 2000 (TRÈS SECRET/ Réservé aux Canadiens)
12. CSE's operational support activities under *** — follow-up – 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)
13. Internal investigations and complaints — follow-up – 10 mai 2000 (SECRET)
14. On findings of an external review of CSE's ITS program – 15 juin 2000 (SECRET)
15. CSE's policy system review – 13 septembre 2000 (TRÈS SECRET/ Réservé aux Canadiens)
16. A study of the *** reporting process — *** (Phase II) – 6 avril 2001 (SECRET/Réservé aux Canadiens)
17. A study of the *** reporting process — *** (Phase III) – 6 avril 2001 (SECRET/Réservé aux Canadiens)
18. CSE's participation *** – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

ANNEXE E : PROGRAMME D'EXAMEN DU BUREAU DU COMMISSAIRE — MODÈLE LOGIQUE



ANNEXE D : ÉTAT DES DÉPENSES, 2010-2011

Sommaire des articles courants

Traitements et salaires	890,939 $
Transports et télécommunications	12,995
Information	21,125
Services professionnels et spéciaux	457,655
Location	170,707
Achat de services de réparation et d'entretien	1,249
Fournitures et approvisionnements	33,252
Acquisition de machine et de matériel	17,500
Total	**1,605,422 $**

ANNEXE C : HISTORIQUE DU BUREAU DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

Le Bureau du commissaire du Centre de la sécurité des télécommunications a été créé le 19 juin 1996, au moment de la nomination du premier commissaire, l'honorable Claude Bisson, O.C., ancien juge en chef du Québec, qui a occupé le poste de commissaire jusqu'en juin 2003. Le très honorable Antonio Lamer, c.p., C.C., c.d., LL.D., d.u., ancien juge en chef du Canada, lui a succédé pour un mandat de trois ans. L'honorable Charles D. Gonthier, C.C., c.r., qui avait pris sa retraite de la Cour suprême du Canada en 2003, a été nommé commissaire en août 2006 et a occupé cette charge jusqu'à son décès en juillet 2009. L'honorable Peter deC. Cory, C.C., c.d., ancien juge de la Cour suprême du Canada, a occupé la charge de commissaire du 14 décembre 2009 au 31 mars 2010. Le 18 juin 2010, l'honorable Robert Décary, c.r., ancien juge de la Cour d'appel fédérale, a été nommé commissaire.

Pendant les six premières années de son mandat (de juin 1996 à décembre 2001), le commissaire a exercé ses fonctions conformément à plusieurs décrets pris en vertu de la partie II de la *Loi sur les enquêtes*. Au cours de cette période, le commissaire a assumé une double responsabilité : examiner les activités du Centre de la sécurité des télécommunications Canada (CSTC) afin de déterminer si elles étaient en conformité avec les lois du Canada, et recevoir les plaintes relatives aux activités du CSTC.

La *Loi antiterroriste* omnibus, qui a été promulguée le 24 décembre 2001, a modifié la *Loi sur la défense nationale* en y ajoutant la partie V.1 et en créant le cadre législatif à la fois pour le Bureau du commissaire et pour le CSTC. Elle confie au commissaire de nouvelles responsabilités relatives à l'examen des activités que mène le CSTC sous le régime d'une autorisation ministérielle et confirme également les pouvoirs du commissaire en vertu de la *Loi sur les enquêtes.*

La Loi omnibus a également introduit la *Loi sur la protection de l'information*, qui remplace la *Loi sur les secrets officiels.* Cette loi attribue au commissaire des fonctions précises dans le cas où une personne astreinte au secret à perpétuité souhaiterait invoquer la défense de l'intérêt public pour justifier la divulgation de renseignements classifiés sur le CSTC.

Le 1er avril 2009, le Bureau du commissaire s'est vu accorder son propre crédit parlementaire. Bien que le commissaire transmette toujours ses rapports au ministre de la Défense nationale, le Bureau est désormais un organisme distinct, qui ne fait plus partie de ce ministère.

(7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.

[...]

273.65 (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.

Loi sur la protection de l'information

15. (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public. [...]

(5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes : [...]

b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession : [...]

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable.

ANNEXE B : MANDAT DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS — EXTRAITS DE LA *LOI SUR LA DÉFENSE NATIONALE* ET LA *LOI SUR LA PROTECTION DE L'INFORMATION*

***Loi sur la défense nationale* – partie V.1**

273.63 (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

ANNEXE A : MANDAT DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS DU CANADA — EXTRAITS DE LA *LOI SUR LA DÉFENSE NATIONALE*

Le Centre de la sécurité des télécommunications du Canada (CSTC) est l'organisme national de cryptologie qui fournit au gouvernement du Canada deux services essentiels : il fournit des renseignements électromagnétiques étrangers et assure la sécurité des technologies de l'information. Le CSTC offre en outre une assistance technique et opérationnelle aux organismes fédéraux chargés de la sécurité et de l'application de la loi.

Les produits et services de renseignement étranger du CSTC sont fournis à l'appui des décisions gouvernementales dans les domaines de la sécurité nationale, de la défense nationale et de la politique étrangère. Ses activités en matière de renseignements électromagnétiques visent exclusivement des renseignements étrangers et sont assujetties aux priorités du gouvernement du Canada en matière de renseignement.

Dans le domaine de la sécurité des technologies de l'information, les produits et services du CSTC permettent aux ministères et organismes gouvernementaux d'assurer la sécurité de leurs systèmes et réseaux d'information électronique. Le CSTC effectue aussi des travaux de recherche et développement au nom du gouvernement du Canada dans des disciplines liées à la sécurité des télécommunications.

Le mandat à trois volets du CSTC est établi au paragraphe 273.64(1) de la *Loi sur la défense nationale*:

a) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;

b) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;

c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère.

Le site Web du CSTC est accessible à : www.cse-cst.gc.ca.

Des récents incidents soulignant la vulnérabilité de nos systèmes informatiques ont ramené le rôle du Centre d'aider à protéger l'information et les infrastructures d'information importantes pour le gouvernement du Canada à l'avant-plan. À cet égard, j'ai demandé à mon équipe d'entreprendre un examen approfondi de ces activités d'importance croissante afin de s'assurer qu'elles se conforment à la loi et protègent la vie privée des Canadiens.

Un mot, en terminant, sur un sujet qui, année après année, revient sur le tapis : le besoin de modifications législatives qui viendront dissiper les ambiguïtés notées par mes prédécesseurs et moi-même dans la *Loi sur la défense nationale*. Je sais que le travail est en cours. J'ose croire que le nouveau gouvernement élu le 2 mai 2011 agira promptement et que les membres du Parlement appuieront l'elimination des ambiguïtés, ce qui, à mon avis, ne devrait soulever aucune controverse.

L'ANNÉE A VENIR

J'entreprends la seconde année de mon mandat avec optimisme et réalisme. Optimisme en raison de la qualité de l'équipe que je dirige, de la rigueur du processus d'examen établi par le Bureau et du professionnalisme qui régit les relations entre le Centre et le Bureau. Réalisme en raison d'un environnement technologique en constante évolution et d'un environnement international tout aussi dynamique auxquels moi-même et mon équipe, ainsi que le Centre, devons nous adapter. Dans ce contexte, je veux m'assurer que le Centre maintient et renforce les mesures prises pour protéger la vie privée des Canadiens.

Notre société libre et démocratique est par ailleurs toujours sujette à des menaces, tant internes qu'externes. Chaque développement technologique dont bénéficie la société a sa contrepartie. Le besoin de réconcilier le droit de tous au maintien d'une société libre et démocratique et le droit de chacun à la protection de sa vie privée exige un effort rigoureux et constant de la part de ceux qui, comme nous, ont le mandat de veiller à ce que les activités des agences qui travaillent dans le plus grand secret se conforment à la loi et protègent la vie privée des Canadiens.

Le besoin de réconcilier le droit de tous au maintien d'une société libre et démocratique et le droit de chacun à la protection de sa vie privée exige un effort rigoureux et constant.

Mon bureau effectuera plusieurs examens au cours de l'année à venir. J'entends porter une attention particulière à ces activités du Centre qui me préoccupent le plus et où les risques d'atteinte à la vie privée sont les plus importants. Je veux m'assurer que le Centre ne conserve aucune communication privée qui ne soit reliée aux affaires internationales, à la défense ou à la sécurité, ce qui est une exigence légale. Je veux aussi m'assurer qu'une identité canadienne ne soit révélée que lorsque cela s'avère strictement nécessaire. Le risque est plus élevé lorsque les informations sont partagées, surtout avec les partenaires internationaux. Aussi ai-je un intérêt particulier pour ce sujet et je ferai rapport l'an prochain d'un examen en cours sur cette question.

PLAN DE TRAVAIL — EXAMENS EN COURS ET PRÉVUS

Les résultats de plusieurs examens actuellement en cours devraient être communiqués au ministre de la Défense nationale au cours de l'exercice à venir et il en sera fait état dans mon rapport annuel 2011-2012.

Les sujets de ces examens sont notamment : un examen annuel des cas mis en évidence par le CSTC en 2010 qui ont eu ou pouvaient avoir des répercussions sur la vie privée d'un Canadien, et les mesures prises par le CSTC pour s'attaquer à cette question; le partage de renseignements étrangers du CSTC avec des partenaires étrangers; l'aide du CSTC au SCRS, en vertu de la partie *c*) du mandat du CSTC et des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité;* et la conservation et la destruction par le CSTC d'informations interceptées, en particulier de communications privées et d'informations concernant des Canadiens.

D'autres examens sont prévus en 2011-2012 qui porteront notamment sur : les activités du CSTC relatives à la sécurité des technologies de l'information menées en vertu des autorisations conférées aux ministères fédéraux par le *Code criminel* et la *Loi sur la gestion des finances publiques*; sur les activités relatives à la sécurité des technologies de l'information menées en vertu d'autorisations ministérielles; et sur certaines activités du centre des opérations du CSTC. Certains examens pourraient être reportés en 2012-2013.

En outre, je poursuivrai les examens annuels des autorisations ministérielles relatives aux renseignements étrangers, de la divulgation par le CSTC d'informations concernant des Canadiens à des clients du gouvernement, et de cas identifiés par le CSTC qui ont eu ou pourraient avoir des répercussions sur la vie privée d'un Canadien ainsi que des mesures prises par le CSTC pour s'attaquer à cette question.

En plus de participer aux séances d'information organisées par le CSTC relativement aux activités que le Bureau du commissaire envisage d'examiner, le Bureau demande au CSTC de préparer des séances d'information reliées à la détermination des risques et à l'élaboration de son plan de travail. Le Bureau reçoit aussi régulièrement des séances d'information concernant les changements touchant la gestion et l'administration des programmes opérationnels du CSTC, notamment ceux relatifs aux politiques et aux procédures.

Formation

En 2010, mon bureau a pris l'initiative de mettre sur pied un atelier sur le processus d'examen destiné au personnel des organisations vouées à l'examen d'organismes d'application de la loi ou d'agences de sécurité et de renseignement. Cet atelier a eu lieu en novembre et a contribué à la formation de personnes appartenant à ces organismes d'examen. L'objectif est d'améliorer l'efficacité de l'examen indépendant. Un autre atelier se tiendra à l'automne 2011.

Mon bureau a pris l'initiative de mettre sur pied un atelier sur le processus d'examen.

Plusieurs membres de mon équipe ont bénéficié d'une formation concernant l'utilisation d'une base de données propre au CSTC dédiée expressément aux renseignements étrangers. Je tiens à remercier le CSTC pour cette opportunité.

Autres activités

En octobre 2010, mon bureau a participé au colloque annuel de l'Association canadienne pour les études de renseignement et de sécurité (ACERS) à Ottawa, qui avait pour thème « Comprendre la sécurité nationale ». D'éminents experts du Canada et d'autres pays ont présenté leurs points de vue concernant des questions importantes pour les milieux de la sécurité, du renseignement et de l'examen.

En décembre 2010, le directeur exécutif de mon bureau et moi-même avons rencontré la commissaire et la commissaire adjointe à protection de la vie privée du Canada pour discuter de nos rôles et responsabilités respectifs. Le directeur exécutif a également participé à un atelier et contribué à l'élaboration d'un guide de référence du Commissariat à la protection de la vie privée du Canada à l'intention des décideurs gouvernementaux.

En mars 2011, le directeur exécutif de mon bureau ainsi que l'ancien président du CPP et la directrice exécutive du CSARS ont participé à une journée de formation s'adressant aux avocats du ministère de la Justice travaillant dans le domaine de la sécurité nationale. Ces derniers ont présenté des exposés sur l'importance de l'examen des organismes d'application de la loi, de sécurité et de renseignement et ils ont animé un débat sur les constatations et les recommandations découlant des enquêtes menées par les honorables juges O'Connor, Iacobucci et Major.

ACTIVITÉS DU BUREAU DU COMMISSAIRE

Comparution devant le Comité permanent de la défense nationale

Comme je l'ai mentionné dans mon introduction, en novembre 2010, j'ai comparu pour la première fois devant le Comité permanent de la défense nationale de la Chambre des communes, qui a examiné ma nomination. J'étais reconnaissant d'avoir la possibilité de rencontrer le Comité si tôt au cours de mon mandat afin de lui faire part de mes expériences et de lui donner un aperçu du cadre législatif du CSTC ainsi que de mon rôle et de mes activités. On peut lire mes remarques devant le Comité sur le site Web de mon bureau au www.ocsec-bccst.gc.ca. J'espère bien avoir d'autres occasions de comparaître devant ce comité ou d'autres pour discuter de mes activités et faire part de mes constatations ou faire valoir l'importance de l'examen de façon générale.

British Intelligence and Security Committee of Parliamentarians

J'ai rencontré les membres du British Intelligence and Security Committee of Parliamentarians lors de leur visite à Ottawa en mars 2011. Les membres du Comité, mon personnel et moi-même avons eu des échanges d'information sur les défis et pratiques à suivre en matière de méthode d'examen. Nous avons comparé les différences dans les modèles respectifs d'examen de nos agences de sécurité et de renseignement.

Forum des organismes de surveillance

Depuis 2005, le Forum des organismes de surveillance réunit des représentants de mon bureau, du Comité de surveillance des activités de renseignement de sécurité (CSARS), du Bureau de l'inspecteur général du Service canadien du renseignement de sécurité, de la Commission des plaintes du public contre la Gendarmerie royal du Canada (CPP) et du Commissariat à la protection de la vie privée du Canada. Le Forum s'est réuni en janvier 2011 pour discuter de questions d'intérêt commun.

- Des politiques et procédures étaient en place pour fournir des consignes suffisantes aux employés du CSTC concernant la protection de la vie privée des Canadiens.
- Les employés du CSTC connaissaient bien les politiques et les procédures et ont agi en conformité avec celles-ci. Les gestionnaires du CSTC ont surveillé les activités pour s'assurer que les employés du CSTC se conformaient aux autorisations en vigueur.
- Je suis convaincu que les pratiques du CSTC et la mise en œuvre prévue d'un nouveau système tiendront compte de ces recommandations et permettront au CSTC de mieux suivre ces activités et de produire des paramètres d'évaluation exacts et uniformes.

Recommandations

Je ne formule aucune recommandation mais je continuerai à effectuer un examen annuel de ces activités pour vérifier si le CSTC continue de se conformer à la loi et adopte des mesures pour protéger la vie privée des Canadiens. Je surveillerai également les efforts déployés par le CSTC pour mettre en œuvre le nouveau système.

PLAINTES CONCERNANT LES ACTIVITÉS DU CSTC

En vertu de mon mandat, je suis tenu d'entreprendre toute enquête jugée nécessaire à la suite d'une plainte – par exemple pour déterminer si le CSTC a mené ou mène une activité non conforme à la loi ou s'il ne prend pas suffisamment de mesures pour protéger la vie privée des Canadiens.

En 2010–2011, aucune plainte justifiant une enquête n'a été reçue.

OBLIGATION SOUS LE RÉGIME DE LA *LOI SUR LA PROTECTION DE L'INFORMATION*

Je suis tenu, en vertu de la *Loi sur la protection de l'information*, de recevoir de l'information émanant de personnes astreintes au secret à perpétuité, qui invoquent la défense de l'intérêt public pour justifier la divulgation de renseignements opérationnels spéciaux. Aucune information de ce genre ne m'a été communiquée en 2010–2011.

Lorsqu'il reçoit une demande subséquente de divulgation de précisions sur l'information supprimée, le CSTC doit vérifier que le ministère ou organisme gouvernemental dont elle émane dispose à la fois de l'autorisation et d'une justification opérationnelle pour obtenir ce genre de renseignements. Ce n'est qu'après que le CSTC peut fournir l'information.

Cet examen a porté sur un échantillon d'environ 20 p. 100 des demandes de divulgation de renseignements supprimés concernant des Canadiens figurant dans les rapports sur les renseignements étrangers, d'avril à septembre 2010. L'échantillon comprenait des renseignements divulgués à tous les ministères et organismes fédéraux qui avaient demandé et obtenu des informations concernant des Canadiens.

Mon bureau a examiné les formulaires utilisés par le CSTC pour documenter l'autorisation et la justification par les ministères et organismes de leurs besoins d'information concernant des Canadiens, de même que les rapports connexes sur les renseignements étrangers.

Bien-fondé de l'examen

Les activités de divulgation du CSTC incluent la communication de renseignements concernant des Canadiens. S'il y avait un cas de non-conformité dans le cadre des activités menées par le CSTC, les répercussions éventuelles sur la vie privée des Canadiens pourraient être importantes.

En outre, j'ai évalué les activités du CSTC en réponse à deux recommandations formulées par mon prédécesseur dans un rapport d'examen de février 2010 demandant que l'on fournisse des outils à l'appui du suivi des demandes des clients et de toute divulgation connexe d'informations supprimées concernant des Canadiens et que l'on renforce la cohérence et l'exactitude des rapports du CSTC au ministre de la Défense nationale concernant ces activités.

Constatations

- D'après l'information dépouillée et les entretiens réalisés, je conclus que la divulgation par le CSTC d'informations supprimées concernant des Canadiens aux clients du gouvernement du Canada avait été faite conformément à la loi.

Recommandations

Les politiques et procédures du CSTC fournissent généralement des consignes suffisantes aux employés du CSTC pour protéger la vie privée des Canadiens tout en déterminant que les entités d'intérêt pour le renseignement étranger sont des entités étrangères situées à l'extérieur du Canada. Toutefois, les politiques et procédures applicables à un certain programme de collecte de renseignements électromagnétiques étrangers ne fournissent qu'une orientation restreinte sur le processus et les pratiques applicables à ces activités. J'ai par conséquent recommandé que le CSTC fournisse des consignes précises concernant ces activités.

À la fin de la période visée par le rapport (le 31 mars 2011), j'attends la réponse du Ministre à cette recommandation. J'en ferai état dans le prochain rapport annuel.

6. Examen annuel de la divulgation par le CSTC de renseignements concernant des Canadiens aux clients du gouvernement du Canada

Contexte

Cet examen donne suite à un engagement pris dans le rapport annuel 2009–2010 de mener un examen annuel portant sur un échantillon de renseignements concernant des Canadiens qui sont divulgués aux ministères et organismes du gouvernement du Canada. L'objet consiste à vérifier si le CSTC se conforme à la loi et applique des mesures pour protéger la vie privée des Canadiens.

Les rapports du CSTC peuvent renfermer de l'information concernant des citoyens canadiens si cette information est essentielle à la compréhension des renseignements étrangers. Toutefois, toute information identifiant un Canadien doit être supprimée des rapports transmis aux ministères et organismes gouvernementaux – c'est-à-dire qu'elle est remplacée par une mention générale du type « un Canadien ».

L'annexe G renferme plus de détails sur les protections législatives au sujet des informations concernant des Canadiens et les communications privées (p. 47).

Les anciens commissaires ont formulé des constatations et des recommandations concernant ces activités, qui nécessitent un suivi. En outre, on a récemment observé d'importants changements touchant certaines technologies ainsi que des politiques et procédures relatives à ces activités, et d'autres sont en cours. Il s'agit de l'un des premiers examens horizontaux approfondis d'un processus du CSTC qui est commun à toutes les méthodes de collecte de renseignement électromagnétique étranger.

Constatations

- D'après l'information dépouillée et les entretiens qui ont été menés, je conclus que le processus en vertu duquel le CSTC détermine les entités d'intérêt pour le renseignement étranger qui sont des entités étrangères situées à l'extérieur du Canada est conforme à la loi, aux exigences ministérielles et aux politiques et procédures du CSTC.
- Le CSTC dispose de politiques et de processus suffisants pour respecter l'obligation en vertu de la loi selon laquelle ses activités d'interception de renseignements électromagnétiques étrangers ne doivent pas cibler des Canadiens quel que soit l'endroit où ils se trouvent dans le monde, ni des personnes au Canada.
- Les employés du CSTC que nous avons interrogés et observés dans leur travail connaissaient bien les politiques et procédures pertinentes et les appliquaient dans leurs activités. Les gestionnaires du CSTC surveillent systématiquement et étroitement les activités pour assurer leur conformité aux autorisations.

Le CSTC s'emploie à concevoir des systèmes pour favoriser la conformité à la loi et la protection de la vie privée des Canadiens.

- Le CSTC s'emploie à concevoir des systèmes et des bases de données connexes pour favoriser la conformité à la loi et la protection de la vie privée des Canadiens. Je conclus que les récentes améliorations apportées à ces systèmes et bases de données aident à assurer la conformité à la loi, et aux exigences ministérielles et aux politiques. Les améliorations supplémentaires prévues renforceront cette conformité.
- J'ai toutefois observé des lacunes dans certains systèmes et bases de données de gestion connexes. Je note avec satisfaction que le CSTC prend des mesures pour corriger ces lacunes et je surveillerai ses efforts à cet égard.

Recommandations

Je n'ai pas formulé de recommandations. Toutefois, du fait que ces activités concernent l'utilisation et l'analyse par le CSTC d'informations concernant des Canadiens, et pourraient, par conséquent, avoir des répercussions sur leur vie privée, j'ai demandé à mon bureau de surveiller ces activités pour s'assurer qu'elles continuent à être exercées conformément à la loi, aux exigences ministérielles et aux politiques et procédures du CSTC.

5. Examen du processus en vertu duquel le CSTC détermine les entités d'intérêt pour le renseignement étranger qui sont des entités étrangères situées à l'extérieur du Canada, comme l'exige la *Loi sur la défense nationale*

Contexte

Le CSTC doit également être en mesure d'identifier les communications privées destinées au Canada ou en provenance du Canada qu'il peut intercepter en toute légalité en vertu d'une autorisation ministérielle selon le principe voulant que l'acquisition de ces communications soit involontaire et que l'interception cible une entité étrangère située à l'extérieur du Canada. Ce processus doit renfermer des mesures pour protéger la vie privée des Canadiens.

Pour la période de septembre 2008 à décembre 2010, j'ai examiné et testé le processus et les pratiques en vertu desquels le CSTC détermine quelles entités d'intérêt pour le renseignement étranger sont des entités étrangères situées à l'extérieur du Canada.

Bien-fondé de l'examen

Ces activités constituent l'assise des programmes de collecte de renseignements électromagnétiques étrangers du CSTC. Des contrôles particuliers sont exercés sur ces activités pour s'assurer qu'elles sont conformes aux obligations en vertu de la loi, aux exigences ministérielles et aux politiques internes du CSTC qui sont essentielles pour protéger la vie privée des Canadiens.

Bien-fondé de l'examen

Ces activités ont trait à l'utilisation et à l'analyse par le CSTC d'informations concernant des Canadiens à des fins de renseignements étrangers. Des contrôles particuliers sont exercés sur ces activités pour assurer la conformité aux obligations en vertu de la loi ainsi qu'aux exigences ministérielles et stratégiques. On a récemment observé d'importants changements touchant certaines politiques, procédures et pratiques. L'examen de ces activités était le premier depuis que le chef du CSTC a permis leur reprise en vertu de nouvelles politiques et procédures. Des questions connexes, des constatations et des recommandations mises en lumière par mes prédécesseurs nécessitaient un suivi.

Constatations

- D'après l'information dépouillée et les entretiens réalisés, je conclus que les activités du CSTC furent autorisées et menées conformément à la loi, aux exigences ministérielles ainsi qu'aux politiques et procédures du CSTC.
- J'ai trouvé que les nouvelles politiques et procédures étaient exhaustives et renfermaient des mesures satisfaisantes pour protéger la vie privée des Canadiens.
- En raison des changements importants apportés par le CSTC à ces activités et des résultats positifs du présent examen, je suis d'avis que le CSTC a donné suite aux constatations et recommandations précédentes.
- Il ressort de mon évaluation que les nouveaux processus mis en place par le CSTC sont conformes à la partie a) de son mandat. Je n'ai pas d'interrogations similaires à celles formulées au cours des années antérieures quant à savoir si de telles activités seraient autorisées de façon plus pertinente en vertu de la partie c) du mandat du CSTC.
- Les nouvelles politiques et lignes directrices ainsi que les nouveaux formulaires du CSTC donnent suite aux constatations et aux recommandations formulées par les anciens commissaires. Les gestionnaires et les représentants du CSTC connaissaient bien les politiques et procédures et s'y sont conformés. Les gestionnaires du CSTC ont surveillé de près ces activités, et ce, régulièrement, pour s'assurer qu'elles étaient conformes aux autorisations.

étrangers. Le CSTC mène ces activités de façon peu fréquente, mais elles peuvent se révéler un outil précieux pour répondre aux priorités du gouvernement du Canada en matière de renseignement. Le CSTC n'a pas besoin d'une autorisation ministérielle pour mener ces activités parce qu'elles n'impliquent pas l'interception de communications privées. Toutefois, une directive ministérielle fournit des orientations sur la façon de les mener.

Ces dernières années, trois examens ont porté jusqu'à un certain point sur ces activités : un examen de la collecte de renseignements étrangers par le CSTC à l'appui de la Gendarmerie royale du Canada (GRC) (Phase II) (2006); un examen des activités du CSTC menées en vertu d'une directive ministérielle (différente) (2008); et un examen de l'appui du CSTC au Service canadien du renseignement de sécurité (SCRS) (2008).

Dans son rapport annuel 2006–2007, feu le commissaire Gonthier se demandait si la partie du mandat du CSTC portant sur les renseignements électromagnétiques étrangers (partie *a*) de son mandat) constituait l'autorisation pertinente dans tous les cas pour permettre au CSTC de donner un appui à la GRC dans la poursuite de ses enquêtes criminelles sur le territoire national. Dans son rapport annuel 2007–2008, le commissaire Gonthier déclarait qu'en attendant un réexamen des questions juridiques soulevées, aucune évaluation ne serait faite de la légalité des activités du CSTC à l'appui de la GRC en vertu de la partie du mandat de l'organisme se rapportant aux renseignements électromagnétiques étrangers. Il a également fait observer que l'appui du CSTC au SCRS soulevait des questions similaires. Le commissaire Gonthier a mis l'accent sur le fait que, même s'il était d'accord avec l'avis que le ministère de la Justice avait fourni au CSTC, il se demandait quelle partie du mandat du CSTC – partie *a*) ou partie *c*), la partie concernant l'asssistance technique et opérationnelle – serait utilisée comme autorisation pertinente pour mener ces activités.

Par suite de ces examens et déclarations dans les rapports annuels, le chef du CSTC a suspendu ces activités. Le CSTC a alors apporté d'importants changements aux politiques, procédures et pratiques connexes.

Recommandations

J'ai formulé trois recommandations dont deux portent sur la communication au ministre de la Défense nationale de certains renseignements se rapportant à la vie privée et sur l'inclusion dans les autorisations ministérielles de l'obligation de faire état de cette information. Cette information est nécessaire pour donner au ministre un tableau complet des activités de collecte du CSTC et pour appuyer le ministre dans sa reddition de comptes pour le CSTC, notamment en ce qui concerne les mesures que prend le CSTC pour protéger la vie privée des Canadiens.

J'ai également recommandé que, compte tenu de l'importance d'assurer la conformité à la loi et la protection de la vie privée des Canadiens, le CSTC devrait accélérer la mise en œuvre d'une politique améliorée de surveillance active des activités menées en vertu des autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers.

À la fin de la période de 2010–2011 visée par le rapport (le 31 mars 2011), j'attendais la réponse du ministre à ces recommandations. J'en ferai état dans le prochain rapport annuel.

4. Examen des activités du CSTC menées en vertu d'une directive ministérielle et visant à identifier de nouvelles entités étrangères d'intérêt pour le renseignement étranger

Contexte

La *Loi sur la défense nationale* investit le CSTC du mandat d'acquérir et d'utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement.

Le CSTC mène plusieurs activités dans le but de repérer de nouvelles sources de renseignements étrangers. Lorsque les autres moyens ont été épuisés, le CSTC peut avoir recours à de l'information concernant des Canadiens s'il a des motifs raisonnables de croire que l'utilisation de cette information pourrait l'aider à découvrir et à obtenir des renseignements

du temps. Ces paramètres éclaireront également le processus d'évaluation du risque et l'élaboration du plan de travail de mes examens.

Un autre objectif de cet examen consistait à analyser un échantillon de communications privées interceptées par le CSTC en vertu des autorisations ministérielles relatives aux renseignements étrangers mais qui n'avaient pas été utilisées dans les rapports du CSTC. L'objet était d'évaluer si cet échantillon renfermait des renseignements étrangers essentiels pour les affaires internationales, la défense ou la sécurité, comme l'exige la *Loi sur la défense nationale*.

Constatations

L'étendue de mon évaluation de la conformité du CSTC à la loi a été déterminée par l'objectif de l'examen, qui était de mettre en évidence et de comprendre les changements importants apportés aux programmes de collecte de renseignements électromagnétiques étrangers.

« le CSTC ne conservait que les communications privées essentielles aux affaires internationales, à la défense ou à la sécurité du Canada. »

- Dans ce contexte, et d'après l'information dépouillée et les entretiens qui ont été menés, je conclus que les activités étaient autorisées en vertu de la *Loi sur la défense nationale* et rien n'indiquait une activité illégale de la part du CSTC. Ce dernier a respecté les exigences ministérielles et il dispose de politiques et de procédures efficaces pour orienter ses activités dans ce domaine.
- On observe des tendances positives dans l'élaboration des politiques, de même que dans la clarté et l'uniformité des demandes d'autorisation ministérielle. Compte tenu du grand nombre de communications interceptées par le CSTC, je conclus que la proportion de communications privées identifiées comme telles qui avaient été interceptées de manière fortuite est demeurée très petite.
- Globalement, les programmes de collecte de renseignements électromagnétiques étrangers n'ont pas changé de façon notable et, en conséquence, j'ai déterminé qu'il n'était pas nécessaire à l'heure actuelle d'effectuer un examen approfondi de ces programmes.
- En ce qui concerne l'échantillon de communications privées, d'après l'information dépouillée et les entretiens, j'ai constaté que le CSTC ne conservait que les communications privées essentielles aux affaires internationales, à la défense ou à la sécurité du Canada, comme l'exige la loi.

3. Examen annuel combiné des activités de collecte de renseignements électromagnétiques étrangers du CSTC menées en vertu d'autorisations ministérielles

Contexte

Il s'agissait du premier examen annuel combiné de l'ensemble des programmes de collecte de renseignements électromagnétiques étrangers. En vertu de la *Loi sur la défense nationale,* je suis tenu d'examiner les activités menées en vertu d'une autorisation ministérielle. Le rapport annuel de 2009–2010 que j'ai présenté au Ministre fait état de la récente adoption d'une nouvelle approche horizontale par le Bureau, qui consiste en un examen approfondi des processus communs à l'ensemble des activités de collecte de renseignements étrangers du CSTC menées en vertu d'une autorisation ministérielle. Par exemple, toutes les méthodes de collecte ont en commun les processus en vertu desquels le CSTC met en évidence, choisit et dirige ses activités portant sur des entités d'intérêt pour les renseignements étrangers; utilise, partage, présente dans des rapports, conserve ou détruit l'information interceptée; et prend des mesures pour protéger les communications privées et l'information concernant des Canadiens. J'ai notamment examiné un rapport de vérification interne du CSTC se rapportant à ces activités.

Bien-fondé de l'examen

L'examen horizontal a conduit à une réévaluation de la façon dont mon bureau analyse les autorisations ministérielles. Comme les processus communs sont examinés dans le cadre des examens horizontaux, il a été déterminé que cet examen annuel combiné des autorisations ministérielles visant les renseignements électromagnétiques étrangers mettrait l'accent sur tous les changements importants et sur toutes les communications privées interceptées de manière fortuite par le CSTC.

Je me suis penché sur les changements apportés aux autorisations et à ceux relatifs à la portée des programmes, à la technologie utilisée par le CSTC et aux cadres de contrôle de gestion connexes. J'ai évalué tous les changements sous l'angle de leur incidence sur le risque pour la conformité à la loi et pour le respect de la vie privée.

J'ai examiné certains paramètres se rapportant à l'interception et à la vie privée des Canadiens. L'objet était d'établir les principales données de référence pour examiner les tendances et pouvoir ainsi cerner tout changement important au fil

Bien-fondé de l'examen

On a récemment observé d'importants changements touchant certaines pratiques et technologies de même que des politiques et procédures du CSTC. Des contrôles particuliers sont exercés sur ces activités pour s'assurer qu'elles sont conformes aux obligations en vertu de la loi, ainsi qu'aux exigences ministérielles et aux politiques du CSTC, et protègent la vie privée des Canadiens. Les anciens commissaires ont également formulé des constatations et des recommandations concernant ces activités. Il s'agit du premier examen depuis la restructuration de ces activités par le CSTC.

Constatations

- D'après l'information dépouillée et les entretiens réalisés, je conclus que les activités du CSTC ont été autorisées et menées conformément à la loi, aux exigences ministérielles et aux politiques et procédures du CSTC.
- J'ai trouvé que les nouvelles politiques et procédures étaient exhaustives et renfermaient des mesures satisfaisantes pour protéger la vie privée des Canadiens.
- Le relevé des activités a montré que le nouveau cadre de contrôle de gestion du CSTC offre de puissants outils de surveillance et de validation de la conformité qui contribuent à assurer la conformité à la loi et la protection de la vie privée des Canadiens.
- Les changements apportés à la technologie et leur application par le CSTC n'ont pas eu d'incidence sur le risque pour la conformité à la loi ou le respect de la vie privée.

Recommandations

Je n'ai formulé aucune recommandation.

- Enfin, cet examen incluait le suivi d'un examen portant sur un logiciel et une base de données d'importance cruciale pour la sécurité des technologies de l'information du CSTC. J'ai confirmé une observation faite l'an dernier dans une étude du Bureau portant sur les activités relatives à la sécurité des technologies de l'information du CSTC exécutées sans autorisation ministérielle, à savoir qu'un logiciel utilisé par le CSTC comporte une fonction adéquate pour limiter l'accès à l'information du système, pour satisfaire aux exigences de sécurité et de confidentialité et pour protéger la vie privée des Canadiens.

Recommandations

Je n'ai formulé aucune recommandation.

2. Examen d'activités relatives à la sécurité des technologies de l'information du CSTC menées en vertu d'une autorisation ministérielle (activité 2)

Contexte

Cet examen portait sur une autre activité relative à la sécurité des technologies de l'information menée pour deux ministères fédéraux, en 2007–2008 et 2008–2009, en vertu d'autorisations ministérielles sous le régime de la *Loi sur la défense nationale*.

Dans le cadre de ces activités, le CSTC tentait de s'introduire dans les systèmes informatiques de ces ministères (dans le cadre d'une simulation contrôlée) afin d'identifier une vulnérabilité potentielle et d'évaluer la réaction des ministères à de telles attaques.

Mon examen révélait notamment des changements à la portée de ces activités et à la technologie utilisée par le CSTC. J'ai évalué ces changements sous l'angle de leurs répercussions possibles sur le risque pour la conformité à la loi et le respect de la vie privée.

Bien-fondé de l'examen

Des contrôles particuliers visant ces activités relatives à la sécurité des technologies de l'information sont en place pour s'assurer qu'elles sont conformes aux obligations en vertu de la loi, ainsi qu'aux exigences ministérielles et stratégiques. Récemment, d'importants changements touchant certaines pratiques ainsi que des politiques et procédures du CSTC se rapportant à ces activités furent observés. Il s'agit du premier examen depuis que le CSTC a restructuré ses activités. Les commissaires précédents ont également établi des constatations et formulé des recommandations sur ces activités.

Constatations

- D'après l'information dépouillée et les entretiens réalisés, je conclus que les activités du CSTC ont été autorisées et menées conformément à la loi, aux exigences ministérielles et aux politiques et procédures du CSTC.
- L'utilisation et la conservation par le CSTC de communications privées et d'informations interceptées de manière fortuite qui concernent des Canadiens ont été conformes à la loi et aux politiques du CSTC.
- Je note avec satisfaction qu'en 2008–2009, le CSTC a apporté d'importants changements aux politiques et aux procédures ainsi qu'au cadre de reddition de comptes visant ces activités. J'estime que les nouvelles politiques et procédures sont exhaustives et renferment des mesures satisfaisantes pour protéger la vie privée des Canadiens.
- Le CSTC a également introduit des procédés qui permettent aux employés de mieux comprendre le cadre de conformité ainsi que les politiques et procédures. Le CSTC a surveillé le déroulement des activités pour vérifier leur conformité aux obligations juridiques et aux exigences ministérielles et stratégiques et il a conservé un registre complet de ces activités.
- J'estime que les changements importants apportés à ces activités relatives à la sécurité des technologies de l'information font suite aux constatations et aux recommandations formulées dans l'examen mené en 2006 par le commissaire.

FAITS SAILLANTS DES SIX EXAMENS SOUMIS AU MINISTRE EN 2010–2011

1. Examen d'activités relatives à la sécurité des technologies de l'information du CSTC menées en vertu d'une autorisation ministérielle (activité 1)

Contexte

La *Loi sur la défense nationale* donne au CSTC le mandat de fournir des avis, des conseils et des services en vue d'aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada.

Cet examen a porté sur certaines activités menées par le CSTC concernant la sécurité des technologies de l'information en vertu d'une autorisation ministérielle en 2008–2009 dans deux ministères fédéraux. Les activités examinées contribuent à protéger les systèmes informatiques en détectant, en analysant et en déjouant des cyberattaques extrêmement complexes visant l'accès secret aux réseaux informatiques sensibles du gouvernement.

Mon examen faisait le suivi d'une question opérationnelle mise au jour à la fin de 2006 qui présentait un risque de non-conformité à la loi. Dans le rapport annuel de 2007–2008, le commissaire avait souligné la façon dont le chef du CSTC avait traité cette question et dont il l'avait tenu ensuite informé des mesures correctives prises.

L'examen comportait également une évaluation des réponses du CSTC aux constatations et recommandations d'un examen antérieur des activités relatives à la sécurité des technologies de l'information menées dans un ministère fédéral donné. Ces constatations et recommandations antérieures se rapportaient aux ambiguïtés dans la politique, la tenue des registres organisationnels et la façon dont les employés du CSTC appréhendaient leurs responsabilités relativement à ces activités. Mon examen incluait également un rapport de vérification interne du CSTC datant de 2007 se rapportant à ces activités.

Les examens précédents portant sur les activités du CSTC exercées en vertu d'autorisations ministérielles montrent de façon uniforme que la proportion de communications privées que le CSTC intercepte de manière fortuite est très petite. Néanmoins, en cas de non-conformité concernant des communications privées, les répercussions éventuelles sur la vie privée des Canadiens pourraient être importantes, et c'est pourquoi je continuerai de me concentrer sur cette activité particulière.

La proportion de communications privées que le CSTC intercepte de manière fortuite est très petite.

L'**annexe G** renferme des renseignements sur les mesures de protection prévues par la loi qui visent les communications privées et l'information concernant des Canadiens (p. 47).

Les résultats

Globalement, je suis en mesure d'affirmer que les activités du CSTC examinées cette année étaient conformes à la loi.

Les examens que j'ai réalisés en 2010–2011 montrent également que :

- le CSTC prend très au sérieux les recommandations du commissaire et y donne suite. Au cours de l'année écoulée, le CSTC s'est attaqué à plusieurs manquements mis en évidence au cours des examens précédents. J'ai été à même de constater en assurant le suivi de ces recommandations que le CSTC avait corrigé ces manquements;

Les activités du CSTC examinées cette année étaient conformes à la loi.

- le CSTC a poursuivi un travail important afin d'intégrer des pratiques de gestion de l'information à ses programmes de base, et a réussi à les intégrer aux activités quotidiennes de ses employés. Il s'agit là d'un élément important qui permet au CSTC de rendre compte de ses activités et de ses décisions; et
- le CSTC dispose de structures de gestion, de gouvernance et de supervision interne bien établies pour orienter et diriger ses activités opérationnelles.

Somme toute, au cours de l'année écoulée, j'ai formulé quatre recommandations. Deux de ces recommandations se rapportent à la présentation d'information au ministre de la Défense nationale dans le but de lui brosser un tableau plus complet des communications que le CSTC intercepte de manière fortuite et qui concernent des Canadiens ou des personnes au Canada. Les deux autres recommandations renforcent l'orientation stratégique de certaines activités du renseignement électromagnétique étranger.

Le CSTC prend très au sérieux les recommandations du commissaire et y donne suite.

APERÇU DES CONSTATATIONS ET DES RECOMMANDATIONS DE 2010–2011

Au cours de l'exercice 2010–2011 visé par ce rapport, j'ai présenté au ministre de la Défense nationale six rapports portant sur mon examen des activités du CSTC.

Ces examens ont été réalisés en vertu de deux volets de mon mandat :

- m'assurer que les activités du CSTC sont conformes à la loi – comme il est stipulé à l'alinéa 273.63(2)a) de la *Loi sur la défense nationale*; et
- m'assurer que les activités du CSTC menées en vertu d'une autorisation ministérielle sont dûment autorisées – comme l'établit le paragraphe 273.65(8) de la *Loi sur la défense nationale*.

Un examen, qui est désormais mené sur une base annuelle, se rapporte aux divulgations d'information concernant des Canadiens aux ministères et organismes du gouvernement du Canada. Cet examen me permet de surveiller étroitement les activités du CSTC lorsqu'il utilise de l'information concernant des Canadiens. L'accomplissement de cet examen annuel me permet de vérifier si le CSTC se conforme à la loi et prend des mesures pour protéger la vie privée des Canadiens.

Deux examens ont porté sur les activités relatives à la sécurité des technologies de l'information du CSTC menées en vertu d'autorisations ministérielles.

Trois examens concernaient les activités de collecte de renseignements électromagnétiques étrangers et incluaient un contrôle de la façon dont le CSTC détermine quelles entités d'intérêt pour le renseignement étranger sont des entités étrangères situées à l'extérieur du Canada, comme l'exige la *Loi sur la défense nationale*.

Recommandations

Depuis 1997, mes prédécesseurs et moi-même avons présenté au ministre de la Défense nationale 61 rapports d'examen et études classifiés. Au total, ces rapports renferment 133 recommandations. Le CSTC a souscrit à 95 p. 100 (122 sur 129) de ces recommandations et il a pris ou prend actuellement des mesures pour y donner suite. J'attends la réponse du ministre aux quatre recommandations formulées en 2010–2011. Au cours de l'année écoulée, le CSTC a terminé le travail donnant suite à trois recommandations antérieures et je surveille de près 18 recommandations que le CSTC s'emploie à mettre en œuvre.

À l'occasion, le CSTC peut rejeter une de mes recommandations. En pareil cas, j'évalue les raisons invoquées de manière à déterminer si elles sont acceptables ou si je dois analyser la question de manière plus approfondie.

L'**annexe F** comprend une liste complète des 61 rapports d'examen et études classifiés présentés au ministre de la Défense nationale (p. 43).

Obligations en vertu de la loi : Je m'attends à ce que le CSTC mène ses activités en conformité avec la *Loi sur la défense nationale*, la *Charte canadienne des droits et libertés,* la *Loi sur la protection des renseignements personnels,* le *Code criminel* et toute autre législation pertinente, et en conformité avec les avis du ministère de la Justice.

Exigences ministérielles : Je m'attends à ce que le CSTC mène ses activités en accord avec les instructions ministérielles, c'est-à-dire conformément à toutes les exigences ou limites précisées dans une autorisation ou une directive ministérielle.

Politiques et procédures : Je m'attends à ce que le CSTC dispose de politiques et de procédures pertinentes pour orienter ses activités et donner des consignes suffisantes sur les obligations en vertu de la loi, les exigences ministérielles et la protection de la vie privée des Canadiens. Je m'attends à ce que les employés soient au courant des politiques et procédures et qu'ils s'y conforment. Je m'attends aussi à ce que le CSTC utilise un cadre de contrôle de gestion efficace pour donner l'assurance qu'il n'y a pas de faille dans l'intégrité de ses activités et leur conformité à la loi. Le CSTC doit être en mesure de rendre compte des décisions prises et de toute information relative à la conformité et à la protection de la vie privée des Canadiens.

Mes rapports d'examen renferment des constatations qui établissent si les critères susmentionnés ont été rencontrés ou non de manière satisfaisante par le CSTC. Ces rapports peuvent également faire état de la nature et de l'importance d'écarts observés par rapport à ces critères. Dans certains cas, je formule des recommandations à l'intention du ministre qui visent à corriger les écarts entre les activités du CSTC et les attentes définies par les critères d'examen. Je surveille les efforts déployés par le CSTC pour donner suite aux recommandations et aux constatations négatives. Je surveille également les champs d'activités des examens antérieurs nécessitant un suivi.

Le modèle logique de l'**annexe E** présente un organigramme de notre programme d'examens exhaustif (p. 41).

Le risque est évalué selon divers facteurs, dont :

- les contrôles associés à l'activité pour assurer la conformité aux obligations légales, aux exigences ministérielles et aux politiques internes du CSTC;
- la question de savoir si l'activité implique des communications privées ou de l'information concernant des Canadiens;
- la nouveauté de l'activité ou le temps écoulé depuis son dernier examen approfondi;
- la survenance d'importants changements touchant les autorisations ou les technologies se rapportant à l'activité;
- le suivi des constatations ou des recommandations se rapportant à l'activité, que les commissaires ont pu formuler; et
- les enjeux qui découlent du domaine public.

Méthode et critères d'examen

« Mon équipe vérifie le contenu des bases de données du CSTC. »

Lorsqu'elle procède à un examen, mon équipe passe en revue les dossiers écrits et électroniques du CSTC, notamment ses politiques et procédures, ainsi que les avis juridiques reçus du ministère de la Justice. Elle compte sur des séances d'information et des présentations offertes par le CSTC relativement à des activités particulières. Elle s'entretient aussi avec des gestionnaires et des employés et elle observe directement les opérateurs et les analystes du CSTC pour vérifier la façon dont ils effectuent leur travail. Mon équipe vérifie l'information recueillie par rapport au contenu des systèmes et des bases de données. Le travail des vérificateurs internes et des évaluateurs du CSTC peut également éclairer les examens.

Chaque examen comporte une évaluation des activités du CSTC selon une série de critères standard, décrits ci-après, relatifs aux obligations légales, aux exigences ministérielles et aux politiques et procédures du CSTC D'autres critères peuvent être ajoutés selon les besoins.

BUREAU DU COMMISSAIRE

Je suis épaulé dans mon travail par un effectif de huit personnes ainsi que par plusieurs experts-conseils recrutés sur une base contractuelle en fonction des besoins. En 2010–2011, les dépenses du Bureau se sont élevées à 1,605,422 $, montant qui ne dépasse pas les limites du crédit alloué par le Parlement.

L'**annexe D** présente l'état des dépenses du Bureau du commissaire du Centre de la sécurité des télécommunications pour 2010–2011 (p. 39).

Objectif de l'examen

L'objectif du processus d'examen rigoureux que mène mon bureau est de me permettre d'assurer au ministre de la Défense nationale et, en fait, à tous les Canadiens, que le CSTC se conforme à la loi et protège la vie privée des Canadiens. Dans l'éventualité où je découvrais un cas où le CSTC ne s'est pas conformé à la loi, je serais tenu d'en informer le ministre de la Défense nationale et le procureur général du Canada.

« L'examen rigoureux me permet d'assurer au ministre que le CSTC se conforme à la loi. »

Sélection des activités visées par l'examen

Les activités du CSTC faisant l'objet d'un examen sont sélectionnées et classées par ordre de priorité en fonction d'une série de critères détaillés qui aident à déterminer les secteurs où le risque de non-conformité à la loi et d'atteinte à la vie privée peut être le plus élevé.

La sélection et la hiérarchisation des sujets visés par un examen sont expliquées dans mon plan de travail triennal, lequel est régulièrement mis à jour dans le cadre d'un processus permanent d'évaluation du risque.

Par ailleurs, je suis tenu chaque année de présenter un rapport sur mes activités au ministre de la Défense nationale, lequel doit ensuite le déposer au Parlement.

Mon bureau est un organisme autonome bénéficiant de son propre crédit parlementaire.

Bien que j'aie pour mandat de faire rapport au ministre, le Bureau du commissaire est indépendant et distinct du ministère de la Défense nationale. L'importance du mandat d'examen qui m'est confié explique le pouvoir dont je suis investi en vertu de la *Loi sur les enquêtes*, ainsi que la nature indépendante de mon bureau, organisme autonome bénéficiant de son propre crédit parlementaire.

L'**annexe B** renferme le libellé des articles pertinents de la *Loi sur la défense nationale* et de la *Loi sur la protection de l'information* se rapportant à mon rôle et à mon mandat en tant que commissaire du CSTC (p. 35) et l'**annexe C** présente l'historique du Bureau du commissaire du Centre de la sécurité des télécommunications (p. 37).

MANDAT DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

Le mandat dont j'ai été investi en vertu de la *Loi sur la défense nationale* comprend trois fonctions principales :

1. **procéder à des examens** concernant les activités du CSTC pour en contrôler la légalité;

2. **faire les enquêtes** que j'estime nécessaires à la suite de plaintes concernant le CSTC; et

3. **informer** le ministre de la Défense nationale et le procureur général du Canada de toute activité du CSTC qui, à mon avis, pourrait ne pas être conforme à la loi.

J'ai en outre pour mandat, en vertu de la *Loi sur la protection de l'information,* de recevoir de l'information émanant de personnes astreintes au secret à perpétuité qui souhaiteraient communiquer des renseignements opérationnels spéciaux en faisant valoir la primauté de l'intérêt public. À ce jour, aucune affaire de ce genre n'a jamais été signalée à un commissaire.

Dans le contexte du mandat du CSTC, l'objet de l'examen consiste :

- à s'assurer que les activités que mène le CSTC en vertu d'autorisations ministérielles sont bien celles autorisées par le ministre de la Défense nationale;
- à s'assurer que le CSTC se conforme à la loi et ne vise que des entités étrangères situées à l'extérieur du Canada;
- à s'assurer que le CSTC applique, de manière efficace, des mesures satisfaisantes de protection de la vie privée des Canadiens dans le cadre de toutes ses activités; et
- à rendre compte des résultats des examens au ministre de la Défense nationale, qui est responsable du CSTC.

Les activités décrites aux parties *a*) et *b*) du mandat du CSTC sont sujettes à trois restrictions législatives visant à protéger la vie privée des Canadiens :

1. Le CSTC se voit interdire par la loi d'exercer des activités qui viseraient des Canadiens – où qu'ils se trouvent dans le monde – ou toute personne au Canada

2. En menant ses activités de collecte de renseignements étrangers ou de protection de la sécurité des technologies de l'information, le CSTC peut intercepter de manière fortuite une communication destinée au Canada ou en provenance du Canada, qui est une communication privée au sens du *Code criminel*. En pareil cas, le CSTC ne peut utiliser ou conserver ces informations que si elles sont essentielles aux affaires internationales, à la défense ou à la sécurité, ou pour mettre en évidence, déterminer ou prévenir des dommages aux systèmes ou aux réseaux informatiques du gouvernement; et

3. Pour l'encadrer formellement, la *Loi sur la défense nationale* exige que l'interception fortuite de communications privées soit autorisée expressément par le ministre de la Défense nationale une fois qu'il est convaincu que les conditions spécifiques définies dans *la Loi sur la défense nationale* sont satisfaites. Ce processus est connu sous le nom d'autorisation ministérielle.

« Le CSTC se voit interdire d'exercer des activités qui viseraient des Canadiens – où qu'ils se trouvent dans le monde – ou toute personne au Canada. »

En apportant son aide en vertu de la partie *c*) de son mandat, le CSTC est assujetti aux mêmes lois et limites régissant les organismes qu'il épaule.

L'**annexe A** renferme le libellé des articles pertinents de la *Loi sur la défense nationale* se rapportant au rôle et au mandat du CSTC (p. 33).

Dès mon entrée en scène, j'ai pris l'initiative de rencontres avec le ministre de la Défense nationale, le chef du Centre, le Conseiller à la sécurité nationale auprès du Premier ministre, le Comité de surveillance des activités de renseignement de sécurité, l'inspecteur général du Service canadien du renseignement de sécurité, la commissaire à la protection de la vie privée et le président par intérim de la Commission des plaintes du public contre la Gendarmerie royale du Canada. Ces rencontres m'ont permis de mieux apprécier à la fois l'ampleur des activités de surveillance des agences de renseignement et de sécurité au Canada et l'opportunité d'un plus grand contact entre les divers organismes de surveillance.

Avant d'expliquer mon rôle, j'aimerais permettre au lecteur de comprendre clairement le mandat du Centre.

MANDAT DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS DU CANADA

La *Loi antiterroriste,* qui est entrée en vigueur en décembre 2001, modifiait la *Loi sur la défense nationale* en lui ajoutant la partie V.1, et définissait comme suit les trois volets du mandat du CSTC :

> La partie *a*) autorise le CSTC à acquérir des renseignements provenant de communications électromagnétiques étrangères à l'appui des priorités du gouvernement du Canada en matière de renseignement;
>
> La partie *b*) autorise le CSTC à aider à protéger l'information électronique et les infrastructures d'information importantes pour le gouvernement du Canada; et
>
> La partie *c*) autorise le CSTC à offrir une aide technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, y compris l'obtention et la compréhension des communications recueillies en vertu des autorisations de ces organismes.

Par ailleurs, j'ai aussi été impressionné, et je dois dire surpris car j'étais au départ sceptique à cet égard, par la transparence et l'esprit de coopération du Centre et de son chef. Il y a eu, déjà, et il y aura encore, c'est sûr, des différends importants, mais dans l'ensemble, je suis à même de constater que la protection de la vie privée des Canadiens est, aux yeux du Centre et de son personnel, une préoccupation beaucoup plus sincère que je ne l'aurais imaginé.

Lors de ma comparution devant le Comité permanent de la défense nationale de la Chambre des communes, le 18 novembre dernier, je faisais état en ces termes du dilemme auquel faisait face le Parlement en adoptant la *Loi antiterroriste* en décembre 2001 :

> Au Canada, chacun a un droit quasi-constitutionnel au respect de sa vie privée. Chacun a aussi un droit constitutionnel à la sécurité de sa personne. Par ailleurs, l'État a l'obligation de protéger l'un et l'autre de ces droits individuels et d'assurer aussi la sécurité du pays. Ces droits et obligations ne sont pas faciles à réconcilier : que serait en effet le droit à la vie privée, que serait le droit à la sécurité de la personne, dans une société dont la sécurité ne serait plus acquise et qui ne serait plus libre et démocratique?

Je dois réconcilier ces droits et obligations dans le contexte bien particulier des activités auxquelles s'adonne le Centre. Il faut rappeler que le premier mandat du Centre est de recueillir des renseignements en provenance d'entités étrangères situées à l'extérieur du Canada. Il est en effet interdit au Centre, de par la loi même qui le constitue, d' « espionner » un Canadien, peu importe où il se trouve dans le monde, ou toute personne au Canada. Ce n'est que de manière fortuite, et j'ajouterais incontournable tant les réseaux globaux de télécommunications sont complexes, omniprésents et tentaculaires, qu'une communication privée est interceptée par le Centre. C'est justement en raison de cette éventualité que la loi permet d'obtenir une autorisation ministérielle. Le nombre de ces interceptions, je m'empresse de le noter, est minime.

MESSAGE DU COMMISSAIRE

J'ai été nommé commissaire du Centre de la sécurité des télécommunications le 18 juin 2010. Je savais très peu de choses du défi qui m'attendait. Je savais que je succédais à d'illustres collègues que j'avais eu le privilège de côtoyer au cours de ma carrière (les juges en chef Bisson et Lamer et les juges Gonthier et Cory). Je savais que je serais impliqué dans un domaine hautement technique et fascinant mais combien délicat, celui de la sécurité et de la protection de la vie privée des Canadiens. J'avais été impliqué, comme avocat puis comme juge d'appel, dans plusieurs dossiers reliés à la vie privée et au terrorisme. Mais jamais je n'aurais imaginé l'ampleur des activités du Centre, non plus que le rôle névralgique du Bureau du commissaire.

D'entrée de jeu je veux saluer l'accueil chaleureux que m'a réservé l'équipe du Bureau du commissaire. Je dis « équipe », car il s'agit d'un groupe de personnes qui travaille dans un esprit de convivialité et de solidarité remarquable. J'ai apprécié tout particulièrement les efforts de vulgarisation qui ont été déployés dès mon arrivée pour me permettre de me familiariser avec les mandats et les rôles respectifs du Bureau et du Centre. À cet égard, je veux remercier le Centre et son chef, John Adams, qui ont fait un effort important pour que je comprenne le plus tôt possible la nature et l'ampleur du travail effectué par le Centre. Les séances d'information que le Centre a préparées à mon intention étaient complexes, intenses et, je dois le reconnaître, bien adaptées à mes besoins.

Au cours de ces premiers neuf mois de mon mandat, j'ai été impressionné par le professionnalisme, l'objectivité et la rigueur de mes analystes. Ils se savent investis d'une mission importante, notamment lorsqu'il s'agit de s'assurer que l'interception fortuite de communications privées concernant des Canadiens est conforme à la loi. Ils ne négligent aucune avenue dans les examens qu'ils effectuent et, s'ils font preuve de réalisme dans un domaine où il n'existe pas de solution miracle, ils ne manifestent pour autant aucune complaisance et passent tout, scrupuleusement, au peigne fin.

Plaintes concernant les activités du CSTC /27

Obligation sous le régime de la *Loi sur la protection de l'information* /27

Activités du Bureau du commissaire /28

Plan de travail — examens en cours et prévus /30

L'année à venir /31

Annexe A : Mandat du Centre de la sécurité des télécommunications du Canada — Extraits de la *Loi sur la défense nationale* /33

Annexe B : Mandat du commissaire du Centre de la sécurité des télécommunications — Extraits de la *Loi sur la défense nationale* et la *Loi sur la protection de l'information* /35

Annexe C : Historique du Bureau du commissaire du Centre de la sécurité des télécommunications /37

Annexe D : État des dépenses, 2010–2011 /39

Annexe E : Programme d'examen du Bureau du commissaire — modèle logique /41

Annexe F : Rapports classifiés au ministre /43

Annexe G : Protection législative visant les communications privées et mesures de protection de l'information concernant des Canadiens /47

TABLE DES MATIÈRES

Message du commissaire /1

Mandat du Centre de la sécurité des télécommunications du Canada /3

Mandat du commissaire du Centre de la sécurité des télécommunications /5

Bureau du commissaire /7

Aperçu des constatations et des recommandations de 2010–2011 /11

Faits saillants des six examens soumis au ministre en 2010–2011 /14

1. Examen d'activités relatives à la sécurité des technologies de l'information du CSTC menées en vertu d'une autorisation ministérielle (activité 1) /14

2. Examen d'activités relatives à la sécurité des technologies de l'information du CSTC menées en vertu d'une autorisation ministérielle (activité 2) /16

3. Examen annuel combiné des activités de collecte de renseignements électromagnétiques étrangers du CSTC menées en vertu d'autorisations ministérielles /18

4. Examen des activités du CSTC menées en vertu d'une directive ministérielle et visant à identifier de nouvelles entités étrangères d'intérêt pour le renseignement étranger /20

5. Examen du processus en vertu duquel le CSTC détermine les entités d'intérêt pour le renseignement étranger qui sont des entités étrangères situées à l'extérieur du Canada, comme l'exige la *Loi sur la défense nationale* /23

6. Examen annuel de la divulgation par le CTSC de renseignements concernant des Canadiens aux clients du gouvernement du Canada /25

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Robert Décary, c.r.

CANADA

Communications Security
Establishment Commissioner

The Honourable Robert Décary, c.r.

Juin 2011

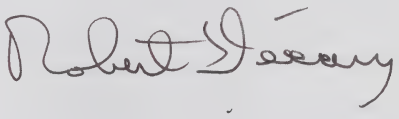
Ministre de la Défense nationale
Édifice MGen G.R. Pearkes, 13e étage
101, promenade Colonel By, tour Nord
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63(3) de la *Loi sur la défense nationale*, j'ai l'honneur de vous transmettre le rapport annuel faisant état de mes activités et constatations pour la période allant du 1er avril 2010 au 31 mars 2011, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Le commissaire,



P.O. Box/C.P. 1984, Station "B"/Succursale « B »
Ottawa, Canada
K1P 5R5
(613) 992-3044 Téléc. : (613) 992-4096

Bureau du commissaire du Centre
de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044
Téléc. : (613) 992-4096
Site Web : www.ocsec-bccst.gc.ca

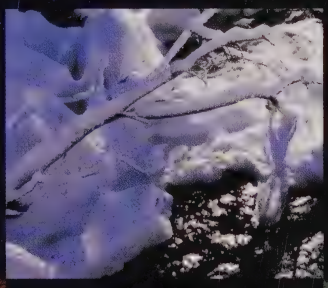
© Ministre des Travaux publics et des
Services gouvernementaux Canada 2011
No de cat. D95-2011

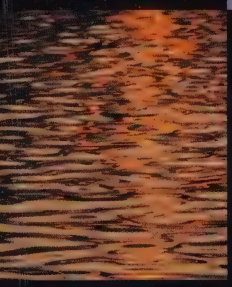
Photo de la couverture : Malak

FSC
www.fsc.org
MIXTE
Papier issu
de sources
responsables
FSC® C103458

Commissaire
du Centre
de la sécurité
des télécommunications

Rapport annuel







2010-2011

Canada

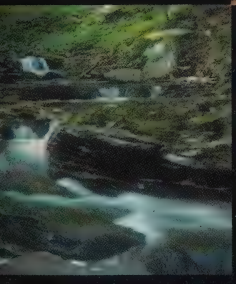
CA1
ND 80D
-S16

Government
Publications

COMMUNICATIONS
SECURITY
ESTABLISHMENT
COMMISSIONER

Annual Report







2011-2012

Canada

Office of the Communications Security
Establishment Commissioner
P.O. Box 1984, Station "B"
Ottawa, Ontario
K1P 5R5

Tel.: 613-992-3044
Fax: 613-992-4096
Website: www.ocsec-bccst.gc.ca

© Minister of Public Works and
Government Services Canada 2012
Cat. No. D95-2012
ISSN 1206 - 7490

Cover photos: Malak

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C103458

Communications Security
Establishment Commissioner

The Honourable Robert Décary, Q.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Robert Décary, c.r.

June 2012



Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Sir:

Pursuant to subsection 273.63(3) of the *National Defence Act*, I am pleased to submit to you my annual report on my activities and findings for the period of April 1, 2011, to March 31, 2012, for your submission to Parliament.

Yours sincerely,

Robert Décary

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

TABLE OF CONTENTS

Biography of the Honourable Robert Décary, Q.C. /2

Commissioner's Message /3

Mandate of the Communications Security Establishment Commissioner /7

Mandate of the Communications Security Establishment Canada /10

Limitations Imposed by Law on CSEC /11

Ministerial Requirements and Policies to Protect the Privacy of Canadians /14

Commissioner's Office and Review Process /18

Overview of 2011–2012 Findings /22

Highlights of the Seven Reviews Submitted to the Minister in 2011–2012 /23

1. CSEC's retention and disposal of intercepted or copied communications /23

2. CSEC's operations centre and particular foreign signals intelligence collection activities conducted in 2010 /25

3. Update on an ongoing review of CSEC's foreign signals intelligence sharing with international partners /26

4. Annual combined review of CSEC foreign signals intelligence ministerial authorizations /28

5. Annual review of a sample of disclosures of Canadian identity information to Government of Canada clients for calendar year 2011 /30

6. and 7. Annual review of incidents identified by CSEC in 2010 and annual review of incidents identified by CSEC in 2011 that affected or had the potential to affect the privacy of Canadians and the measures taken by CSEC to address them /32

Complaints About CSEC's Activities /34

Duty Under the *Security of Information Act* /34

Activities of the Commissioner's Office /35

Work Plan — Reviews Under Way and Planned /37

The Upcoming Year /38

Annex A: Excerpts from the *National Defence Act* and the *Security of Information Act* Related to the Mandate of the Communications Security Establishment Commissioner /41

Annex B: History of the Office of the Communications Security Establishment Commissioner /45

Annex C: Excerpts from the *National Defence Act* Related to the Mandate of the Communications Security Establishment /47

Annex D: 2011–2012 Statement of Expenditures /49

Annex E: Commissioner's Office Review Program — Logic Model /50

BIOGRAPHY OF THE HONOURABLE ROBERT DÉCARY, Q.C.

The Honourable Robert Décary, Q.C., was appointed Commissioner of the Communications Security Establishment on June 18, 2010.

Commissioner Décary was born in Montréal in 1944. He received his education at Collège Jean-de-Brébeuf (BA), at Université de Montréal (LL.L.) and the University of London (LL.M.). He was called to the Québec Bar in 1967 and named Queen's Counsel in 1986.

In the course of a career dedicated to public office, the law and journalism, he was Special Assistant to the Honourable Mitchell Sharp (then Canada's Secretary of State for External Affairs) (1970–1973), Co-Director for Research on the Task Force on Canadian Unity, the Pepin-Robarts Commission (1978–1979) and member of the French Constitutional Drafting Committee of the Federal Department of Justice (1985–1990).

He practised law in Montréal, then in Gatineau, where, in the firm Noël, Décary, he specialized in representing many law offices and the Attorney General of Québec before the Supreme Court of Canada.

He has written a number of feature articles for *Le Devoir* and *La Presse*, and has contributed to many legal journals and textbooks. He is the author of *Aide-mémoire sur la Cour suprême du Canada* (1988) and of *Chère Élize* (or *The Long and the Short History of the Repatriation*) (1983).

He was a member of the Federal Court of Appeal from 1990 to 2009. In 2009, he was appointed arbitrator of the Court of Arbitration for Sport in Lausanne, and in 2010 he became a member of the Sport Dispute Resolution Centre of Canada.

COMMISSIONER'S MESSAGE

The primary purpose of this report is to inform the Minister of National Defence of my activities during the fiscal year ending March 31, 2012. I will make mention of the results of reviews I conducted into the operations of the Communications Security Establishment Canada (CSEC) during the past year, as well as review projects currently under way and those that I expect to undertake in the next few months. I will also refer to other activities that I and my office have conducted, especially those meant to keep us abreast of the latest developments in Canada and abroad in the area of review of security and intelligence agencies.

Two-thirds of the way through my three-year mandate, I am obliged to note that the public, and sometimes even so-called experts, continue, because of a lack of knowledge, to misjudge the respective roles of Canada's various intelligence agencies and, consequently, those of the various review bodies. There is a reason for this ignorance. The secret nature of the activities of intelligence organizations is such that any attempts at educating the public come up against a culture of silence that makes one keep quiet even about what is known or what could be made known. To paraphrase a well-worn expression, the fear that one might see certain trees is such that one is not allowed to describe the forest. In my opinion, it is possible, without going into details it would be inappropriate to divulge, to employ simpler and more comprehensible language and thus ensure that public debates are not held on false premises.

In my message of last year, I briefly described my own mandate and that of CSEC. This year, I shall be revisiting this in greater detail in my report.

Technology is developing at a staggering pace. CSEC's expertise in communications technology results in its providing assistance, pursuant to its mandate, to other members of Canada's security and intelligence community, particularly the Canadian Security Intelligence Service (CSIS). This year, as I pursue my efforts to inform the public through

this report, I would like to better define the respective roles of CSEC and CSIS. I find that these roles are frequently misunderstood.

When acting on its own initiative, CSEC does not have the right, under its enabling legislation, to target anyone within Canada or any Canadian outside Canada. However, CSEC also has a mandate to lend assistance to such organizations as CSIS, which might, upon request, lead to an involvement with a Canadian or someone on Canadian soil. In providing such assistance, CSEC is subject to the laws governing the organization that has made the request.

Since CSIS, under its enabling legislation, is concerned with threats to the security of Canada and may conduct its investigations using methods including the interception of private communications, the invasion of the privacy of Canadians is inherent in these activities, and Parliament wanted these activities to take place only upon the securing of a judicial warrant. Accordingly, when CSIS is executing such a warrant and requests the assistance of CSEC, CSEC is in effect simply taking part in an activity already authorized by a court. It would be superfluous to require another warrant at that point. My predecessors have reviewed the assistance provided to CSIS by CSEC. This year, I undertook an in-depth review, which I will complete in the next few months, of certain activities in which CSEC acts on a request of CSIS.

Furthermore, since CSEC is only authorized to target non-Canadians outside Canada, any interception of private communications involving Canadians is as unintentional as it is unforeseeable. Therefore, Parliament has required that these activities of CSEC that could unintentionally breach the privacy of Canadians be the object, not of a warrant, but of a ministerial authorization issued by the Minister of National Defence. This ministerial authorization, however, does not amount to a blank cheque; it comes with significant requirements, some legal and others that the Minister may prescribe, to ensure that, should the privacy of a Canadian become involved, measures are in place to protect it.

Increased cooperation between CSEC and CSIS in turn requires increased cooperation between the organizations that review them. This is not easily done, as the laws governing review bodies set up highly compartmented competencies that do not encourage pooling energies and resources. Lately, I have been working on finding ways of making the reviews that my office and the Security Intelligence Review Committee (SIRC) each undertake more complementary, to satisfy myself that no activities of CSEC and CSIS elude review. Paragraph 273.63(6) of the *National Defence Act* allows the Governor in Council to authorize me to engage in any related activity. Article 54 of the *Canadian Security Intelligence Service Act* allows the Minister of Public Safety and Emergency Preparedness to request from SIRC a "special report concerning any matter that relates to the performance of its duties and functions". I am of the opinion that my office and SIRC could, by virtue of these provisions, be asked to conduct a joint review or complementary reviews of certain activities involving both CSEC and CSIS. This approach would be squarely in keeping with the recommendations formulated by Justice Dennis O'Connor, in his second report of the *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar*, on the system for reviewing security and intelligence organizations in Canada.

This annual report would not be complete if I did not highlight certain major changes in the top management of CSEC and in its status.

Last January, John Adams, who had been Chief of CSEC for six years, was appointed as Senior Advisor to the Privy Council Office and as Skelton-Clark Fellow to the Queen's University School of Policy Studies. I am in a position to testify just how much he was able to develop a culture of respect for privacy within CSEC. There will, of course, always be an inevitable and necessary climate of tension between a review body and the organization being reviewed. The challenge, then, for the heads of the two organizations is to make sure this tension is business-like and productive. To my mind, this has been the case.

John Forster, a seasoned senior civil servant, assumed leadership of the CSEC on January 30, 2012. I have met with him on several occasions and I already discern in him the traits of his predecessor. I am confident that our relationship will be marked by courtesy and respect. My team and I organized an intensive information session for the new Chief in order to present him with the clearest possible picture of how I carry out my review mandate under the Act.

Incidentally, until November 16, 2011, CSEC had been under guardianship of a sort, reporting both to the Deputy Minister of National Defence for its administration and finances and to the National Security Advisor to the Prime Minister for its operations and policies. On that day, CSEC became an autonomous body in the National Defence Minister's portfolio with departmental status. Its Chief acquired the rank of Deputy Head and reports directly to the Minister.

I do not expect this change of status to have any impact on the relationship between my office and CSEC. However, I am of the view that the requirement to report to the National Security Advisor to the Prime Minister allowed a broader government perspective on national security to be applied to CSEC operations and policies, and I will be watchful whether CSEC's new autonomy results in any weakening of its accountability and compliance control framework.

MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

Overview

- My mandate (and CSEC's) is set out in Part V.1 of the *National Defence Act*.
- I operate at arms-length from government.
- I submit detailed classified reports of my reviews of CSEC to the Minister of National Defence.
- My recommendations aim to reduce risks of non-compliance with the law by CSEC and to strengthen its practices to protect the privacy of Canadians.

My mandate under the *National Defence Act* consists of three key functions:

1. **reviewing CSEC activities** to ensure they comply with the law;

2. **conducting investigations** I deem necessary in response to complaints about CSEC; and

3. **informing the Minister** of National Defence and the Attorney General of Canada of any CSEC activities that I believe may not be in compliance with the law.

Under the *Security of Information Act*, I also have a mandate to receive information from persons who are permanently bound to secrecy if they believe it is in the public interest to release special operational information of CSEC. To date, no such matters have been reported to a Commissioner.

Reviewing CSEC activities

The purpose of my review mandate is:

- to ensure that activities conducted by CSEC under ministerial authorization are, in fact, those authorized by the Minister of National Defence;
- to ensure that CSEC complies with the law and, if I believe that it may not be complying, to report this to the Minister of National Defence and to the Attorney General of Canada;
- to ensure that CSEC does not direct its foreign signals intelligence and information technology (IT) security activities at Canadians; and
- to ensure that CSEC develops and effectively applies satisfactory measures to protect the privacy of Canadians in all the activities it undertakes.

Conducting investigations

My mandate includes undertaking any investigation I deem necessary in response to a written complaint — for example to determine whether CSEC has engaged, or is engaging, in unlawful activity or is not taking sufficient measures to protect the privacy of Canadians.

Once a written complaint is received, if I determine that it has merit and relates to my mandate, I have all the powers of a Commissioner under Part II of the *Inquiries Act* to access and review any information held by CSEC. I may also interview — under oath, if necessary — any CSEC employee to establish the facts concerning a complaint. I advise the complainant, the Minister of National Defence and the Chief of CSEC about the results of a formal complaint investigation. If I believe that CSEC may not have complied with the law, I would report this to the Minister and to the Attorney General of Canada.

Informing the Minister

Under my mandate, I also:

- report the results of my reviews, in classified reports, to the Minister of National Defence, who is accountable to Parliament for CSEC; and
- am required to submit an unclassified report to the Minister of National Defence on my activities each year, which the Minister must then table in Parliament. This is the 16th annual report.

My reviews focus on CSEC's compliance with its legal, ministerial and policy requirements. While it is my primary duty to report any non-compliance by CSEC, a necessary element of my mandate also includes informing CSEC of any activities that I believe might present, or have the potential to present, a risk of non-compliance, such as an unlawful interception of a private communication or other invasion of the privacy of a Canadian. If I am not satisfied that CSEC is responding to my concerns appropriately, I have the authority and the duty to report them to the Minister of National Defence. A number of my reports have included recommendations aimed at prevention. It is my goal to strengthen CSEC practices that contribute to compliance and incorporate measures that protect the privacy of Canadians. I believe it is ultimately more useful to prevent unlawful activity than to identify it after the fact.

Independence

While I submit my reports to the Minister responsible for CSEC, my office is independent and separate from the Department of National Defence. My review mandate is supported by the powers I have under the *Inquiries Act*. These powers ensure my access to all CSEC information and employees and include the power of subpoena. The independence of my mandate is further supported by the way my office is funded — it has been allocated its own appropriation from Parliament rather than receiving funding from the Department of National Defence.

Annex A contains the text of the relevant sections of the *National Defence Act* and the *Security of Information Act* relating to my role and mandate as CSE Commissioner (p. 41). **Annex B** describes the history of the Office of the CSE Commissioner (p. 45).

MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

When the *Anti-terrorism Act* came into effect on December 24, 2001, it added Part V.1 to the *National Defence Act*, and set out CSEC's three-part mandate:

> Part (a) authorizes CSEC to acquire and use foreign signals intelligence in accordance with the Government of Canada's intelligence priorities;
>
> Part (b) authorizes CSEC to help protect electronic information and information infrastructures of importance to the Government of Canada; and
>
> Part (c) authorizes CSEC to provide technical and operational assistance to federal law enforcement and security agencies, including helping them obtain and understand communications collected under those agencies' own authorities.

Protection of Canadians

CSEC is prohibited by law from directing its foreign signals intelligence collection and IT security activities at Canadians — wherever they might be in the world — or at any person in Canada.

LIMITATIONS IMPOSED BY LAW ON CSEC

Parts (a) and (b) of CSEC's mandate

CSEC's activities related to the collection of foreign signals intelligence and to the protection of electronic information and information infrastructures of importance to the Government of Canada are subject to three legislative limitations aimed at protecting Canadians' privacy:

1. CSEC is prohibited from directing its foreign signals intelligence collection and IT security activities at Canadians, regardless of their location anywhere in the world, or at any person in Canada, regardless of their nationality;

2. In conducting these activities, CSEC may unintentionally intercept a communication that originates or terminates in Canada in which the originator has a reasonable expectation of privacy, which is a "private communication" as defined by the *Criminal Code*. CSEC *may* use and retain a private communication obtained this way but *only* if it is essential to either international affairs, defence or security, or to identify, isolate or prevent harm to Government of Canada computer systems or networks; and

3. To provide a formal framework for the unintentional interception of private communications while conducting foreign signals intelligence collection or IT security activities, the *National Defence Act* requires express authorization by the Minister of National Defence. These are known as ministerial authorizations. The Minister may authorize the activities once he or she is satisfied that specific conditions provided for in the Act have been met, which includes assurances of how such unintentional interceptions of private communications would be handled should they arise.

Private Communication: "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it" (section 183 of the *Criminal Code*).

Ministerial authorizations

When CSEC is conducting activities to acquire foreign signals intelligence, it cannot know beforehand with whom a targeted foreign entity outside Canada may communicate. Similarly, when CSEC is conducting activities to help protect Government of Canada computer systems, it cannot know beforehand who may communicate with or through that computer system. Given the complexity and interconnectedness of the global information infrastructure, it is unavoidable that CSEC will intercept a number of private communications. It is for this reason that CSEC requires a ministerial authorization for these activities — to shield itself from the *Criminal Code* in cases where it may unintentionally intercept a communication coming to or originating from Canada and where a person has an expectation of privacy. CSEC's ministerial authorizations relate to an "activity" or "class of activities" specified in the authorizations — that is, to a specific method of acquiring foreign signals intelligence or of protecting computer systems (the how); the authorizations do not relate to a specific individual or subject (the whom or the what).

Conditions for ministerial authorizations

To issue a ministerial authorization for foreign signals intelligence collection, the Minister must first be satisfied that:

- the interception will be directed at foreign entities located outside of Canada;
- the information could not be reasonably obtained by other means;
- the expected value of the interception would justify it; and
- satisfactory measures are in place to protect the privacy of Canadians and private communications will only be used or retained when essential to international affairs, defence or security.

To issue a ministerial authorization to protect the computer systems or networks of the Government of Canada, the Minister must be satisfied that:

- the interception is necessary;
- the information could not be reasonably obtained by other means;
- the consent of persons whose private communications may be intercepted could not reasonably be obtained;
- satisfactory measures are in place to ensure that only information essential to identify, isolate or prevent harm to Government of Canada computer systems or networks will be used or retained; and
- satisfactory measures are in place to protect the privacy of Canadians in the use and retention of that information.

Ministerial authorization: authorization provided in writing by the Minister of National Defence to CSEC so that CSEC is not in contravention of the *Criminal Code* if — in the conduct of foreign signals intelligence collection or IT security activities — it should unintentionally intercept a private communication. An authorization can be in effect for no longer than one year. In 2011–2012, there were six foreign signals intelligence collection and two IT security ministerial authorizations in effect.

Each year, I review all of CSEC's ministerial authorizations — which may be in effect for a period of no longer than one year — to ensure that the activities are authorized and that the above conditions for authorization are met. I report to the Minister of National Defence on my review.

Part (c) of CSEC's mandate

For CSEC to provide assistance to federal law enforcement and security agencies in fulfilling their mandated activities, the *National Defence Act* requires that those agencies first demonstrate that they have the legal authority — such as an authorization or a warrant — to conduct the activities. CSEC is then subject to the same laws and limitations that govern the agencies it is assisting rather than to the three legislative limitations listed above. In addition, ministerial authorizations do not apply to these activities.

MINISTERIAL REQUIREMENTS AND POLICIES TO PROTECT THE PRIVACY OF CANADIANS

CSEC's foreign signals intelligence and IT security activities are subject to measures, in addition to the limitations in the *National Defence Act*, that protect the privacy of Canadians in the use and retention of intercepted information.

Both CSEC's foreign signals intelligence and IT security program areas have dedicated sections responsible for day-to-day compliance and oversight. These two sections are important components of CSEC's management monitoring and accountability frameworks, and I examine their effectiveness as part of my reviews.

Handling of intercepted private communications

CSEC should use available means to reduce, to the extent possible, the unintentional interception of the private communications of Canadians. But what happens when CSEC's foreign signals intelligence and IT security activities result in unintentionally intercepted private

communications? If such unintentional interception does occur, these communications and information must be destroyed unless:

- they consist of foreign intelligence as defined in the *National Defence Act* and in accordance with the Government of Canada intelligence priorities;
- are essential to protect the lives or safety of individuals of any nationality;
- contain information on serious criminal activity relating to the security of Canada; or
- are essential to identify, isolate or prevent harm to Government of Canada computer systems or networks.

When ministerial authorizations expire, the Chief of CSEC must report to the Minister of National Defence information on the private communications unintentionally intercepted. These reports must state how many private communications were used or retained — on the basis, as required by law, that they are essential to international affairs, defence or security, or essential to identify, isolate or prevent harm to Government of Canada computer systems or networks. These reports must also include the number and value of any foreign intelligence reports produced from the intelligence derived from the private communications.

I examine the Chief's reports to the Minister, monitor the number of private communications unintentionally intercepted, and verify how CSEC treated and used these communications. I am able to review all of the private communications that CSEC uses and retains.

Directives and policies

Ministerial directives contain written direction to the Chief of CSEC on the Chief's duties and CSEC's activities. The June 2001 Ministerial Directive on *Communications Security Establishment Accountability Framework* sets out the accountability regime for CSEC, including a requirement for CSEC to report annually to the Minister of National Defence on CSEC's priorities and initiatives as

well as legal, policy and management issues of significance. The Chief's reports are one way I keep abreast of CSEC's activities. They also inform the development of my review work plan.

One ministerial directive in particular, the June 2001 Ministerial Directive on *Privacy of Canadians*, reinforces the requirements in the *National Defence Act* and ministerial authorizations. It requires CSEC to adopt measures to minimize the unintentional interception of private communications. It states that CSEC may retain and report information on or of Canadians, subject to specific criteria and appropriate measures in place for the handling, retention and destruction of this information. The treatment of this information must be consistent with the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*. Other ministerial directives provide guidance on specific CSEC activities.

CSEC's operational policy, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, applies to anyone conducting activities under CSEC authority, including CSEC employees and military personnel. It contains detailed measures for legal compliance and to safeguard the privacy of Canadians in the use and retention of intercepted information. Many other policies and procedures contain detailed requirements and provide instructions on specific CSEC activities and on measures to protect privacy. I review CSEC's activities to ensure compliance with ministerial directives and policies and procedures.

Information about Canadians: any personal information (as described in the *Privacy Act*) about a Canadian, including a Canadian corporation.

Canadian identity information

CSEC's reports may contain Canadian identity information, if that information is deemed essential to understand the reports. However, the reference to an identified Canadian must be suppressed and replaced by a generic reference such as "a named Canadian" person or company. When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC must verify that the requesting government department or agency has both the authority and the operational justification for obtaining the Canadian identity information. Only then may CSEC provide this information. Annually, I select and review a sample of these disclosures to verify that CSEC complies with the law and maintains measures to protect the privacy of Canadians.

International collaboration

CSEC and its closest international partners — the United States' National Security Agency, the United Kingdom's Government Communications Headquarters, the Australian Defence Signals Directorate, and the New Zealand Government Communications Security Bureau — respect each other's laws by pledging not to target one another's citizens' communications. CSEC is prohibited from requesting an international partner to undertake activities that CSEC itself is legally prohibited from conducting. My reviews examine CSEC's cooperation with its allies to ensure compliance with the law.

CSEC training

CSEC's training program helps to ensure staff awareness of requirements and policies relating to lawfulness and the protection of the privacy of Canadians. Every new CSEC employee attends a foundational learning course, the curriculum of which includes information on legal and policy requirements and mandatory measures to protect privacy. For certain operational activities, CSEC's employees are required to participate in briefings on legal requirements prior to conducting the activities and at least yearly thereafter. During my reviews, I determine the extent to which this training is effective by questioning CSEC employees about their understanding of the requirements. **Annex C** contains text of relevant sections of the *National Defence Act* relating to the role and mandate of CSEC (p. 47).

COMMISSIONER'S OFFICE AND REVIEW PROCESS

I am supported in my work by a staff of eight, together with a number of subject-matter experts, under contract, as required. In 2011–2012, my office's expenditures were $1,942,429, which is within the budget provided by Parliament. An expansion to the physical space of my office is under way, which will allow me to hire additional employees.

Annex D provides the 2011–2012 Statement of Expenditures for the Office of the Communications Security Establishment Commissioner (p. 49).

Objective of review

The objective of my review is to enable me to provide to the Minister of National Defence, and indeed to all Canadians, assurance that CSEC is complying with the law and protecting the privacy of Canadians. If I were to find an instance where I believe CSEC may not have complied with the law, it would be my duty to inform the Minister of National Defence and the Attorney General of Canada.

Selection of activities for review

I use a risk-based and preventative approach to my reviews. I have a three-year work plan, which is updated twice per year. I draw on many sources to develop my work plan. My employees and I receive regular briefings from CSEC on new activities and on changes to existing activities of CSEC. I also go over the Chief of CSEC's annual report to the Minister of National Defence on CSEC's priorities and initiatives as well as legal, policy and management issues of significance. I then use a set of criteria to help select and prioritize CSEC activities based on where risk is greatest for potential non-compliance with the law including for risks to the privacy of Canadians.

Risk is assessed by considering, among other factors:

- the controls placed by CSEC on the activity to ensure compliance with legal, ministerial and policy requirements;
- whether the activity has the potential to involve private communications or information about Canadians;
- whether the activity is new, has changed significantly, or has had a lengthy period elapse since its last in-depth review;
- whether there have been significant changes to the authorities or technologies relating to the activity;
- whether Commissioners have made findings or recommendations relating to the activity that require follow-up; and
- issues arising in the public domain.

Review methodology and criteria

In conducting a review, my office examines CSEC's hard-copy and electronic information and records, as well as CSEC's policies and procedures and legal advice received from Justice Canada. My staff request briefings and demonstrations of specific activities, interview managers and employees and observe CSEC operators and analysts first hand to verify how they conduct their work. My staff test information obtained against the contents of systems and databases. The work of CSEC's internal auditors and evaluators may also inform reviews.

Each review includes an assessment of CSEC's activities against a standard set of criteria, described below, consisting of legal requirements, ministerial requirements, and policies and procedures. Each review may have additional criteria added, as appropriate.

> **Legal requirements**: I expect CSEC to conduct its activities in accordance with the *National Defence Act*, the *Privacy Act*, the *Criminal Code*, the *Canadian Charter of Rights and Freedoms* and any other relevant legislation, and in accordance with Justice Canada advice.

Ministerial requirements: I expect CSEC to conduct its activities in accordance with ministerial direction, following all requirements and limitations set out in a ministerial authorization or directive.

Policies and procedures: I expect CSEC to have appropriate policies and procedures in place to guide its activities and to provide sufficient direction on legal and ministerial requirements including the protection of the privacy of Canadians. I expect employees to be knowledgeable about and comply with policies and procedures. I also expect CSEC to employ an effective management control framework for maintaining the integrity and lawful compliance of its activities. This includes appropriate accounting for decisions taken and for information relating to compliance and the protection of the privacy of Canadians.

My review reports document CSEC's activities and practices and contain findings relating to the above-noted criteria. These reports may also disclose the nature and significance of deviations from the criteria. In some cases, I make recommendations to the Minister that are aimed at correcting discrepancies between CSEC's activities and the expectations established by the review criteria. I monitor how CSEC addresses recommendations and responds to negative findings. As well, I monitor areas for follow-up identified in past reviews.

The process of review is cumulative. Since my office was established in 1996, it has built up specific expertise in CSEC's unique mandate and activities. With each review my office adds to its knowledge of CSEC's activities and of how we can improve our own methodology. One such change implemented in recent years by my office was the introduction of horizontal reviews — that is, review of the processes by which CSEC selects foreign intelligence targets and uses, shares, reports, retains or disposes of intercepted information that are common to each of the activities or class of activities. This approach has provided for greater

depth of review. My office examines each of these common processes to determine whether CSEC complies with the law and the extent to which CSEC takes measures to protect the privacy of Canadians.

The Logic Model in **Annex E** provides a flow chart of our comprehensive review program (p. 50).

Horizontal reviews examine processes common to all CSEC foreign signals intelligence collection methods or IT security activities under ministerial authorization. For example, the processes by which CSEC:

- identifies, selects and directs its activities at entities of foreign intelligence interest;
- uses, shares, reports, retains or disposes of intercepted information; and
- takes measures to protect private communications intercepted unintentionally and Canadian identity information.

Recommendations

Since 1997, my predecessors and I have submitted to the Minister of National Defence 68 classified review reports. In total, the reports contained 133 recommendations. CSEC has accepted and implemented or is working to address 93 percent (124 out of 133) of these recommendations. Recommendations have contributed to CSEC suspending certain activities to re-examine how the activities are conducted and to restructure the processes and practices supporting the activities. This past year, CSEC completed work in response to one past recommendation and I am monitoring 15 recommendations that CSEC is working to address. I continue to await the Minister's response to one privacy-related recommendation I made in 2010–2011.

My website provides a complete list of the 68 classified review reports submitted to the Minister of National Defence (www.ocsec-bccst.gc.ca).

OVERVIEW OF 2011–2012 FINDINGS

During the 2011–2012 reporting year, I submitted seven reports to the Minister of National Defence on my review of CSEC activities.

These reviews were conducted under two areas of my mandate:

- ensuring CSEC activities are in compliance with the law — as set out in paragraph 273.63(2)(*a*) of the *National Defence Act*; and
- ensuring CSEC activities under a ministerial authorization are authorized — as set out in subsection 273.65(8) of the *National Defence Act*.

The results

Each year I provide a statement on my findings about the lawfulness of CSEC's activities in general. Overall, I am able to report that the activities of CSEC examined this year complied with the law. I made no recommendations this year. However, I made a number of suggestions to improve certain policies and practices the application of which I will be monitoring.

In some ways, it was a frustrating year due to delays in being able to proceed with some reviews. CSEC did not provide the same level of support to my office for these reviews, resulting in excessive delays. It has committed to correcting this situation. Ministerial direction requires the Chief of CSEC to support the Commissioner's reviews.

HIGHLIGHTS OF THE SEVEN REVIEWS SUBMITTED TO THE MINISTER IN 2011–2012

1. CSEC's retention and disposal of intercepted or copied communications

Background

The ever-increasing amount of electronic information being generated in our interconnected world has created challenges for CSEC in managing the retention (storage) and disposal (destruction) of the information it acquires. CSEC's foreign signals intelligence and IT security programs recently made significant technological changes impacting on their respective retention and disposal practices for acquired communications.

Paragraph 273.64(2)(*b*) of the *National Defence Act* requires CSEC to take measures to protect the privacy of Canadians. It includes the manner in which CSEC retains and disposes of communications that it intercepts in the conduct of its foreign signals intelligence collection and IT security activities. In this review, I paid particular attention to CSEC's retention and disposal of unintentionally intercepted private communications and Canadian identity information.

As a Government of Canada institution, CSEC also has a legal requirement to keep certain records. The *Access to Information Act* and the *Privacy Act* both recognize that citizens have the right, under specified conditions, to access government records. Federal institutions, such as CSEC, must also protect any personal information that they may collect or transmit. These legal requirements reinforce the obligation for CSEC to maintain a comprehensive and complete inventory and description of its information holdings. The unauthorized destruction of a record could result in an inability to document an activity, and consequently, an inability to demonstrate compliance.

My predecessors and I have always monitored CSEC's information management practices because the creation and retention of records is one of the main means by which CSEC can account for its activities and

provide assurance that its activities comply with legal, ministerial and policy requirements. My predecessors made a number of recommendations that resulted in significant developments in CSEC's information management practices and related systems to strengthen compliance.

Findings

I found that both CSEC's foreign signals intelligence collection and IT security programs have incorporated into the digital architectures of their respective programs a number of legal, ministerial and policy requirements relating to retention and disposal. I acquired detailed knowledge of and documented this policy-based and technology-assisted approach to CSEC information management practices. During this review, I found that CSEC built a number of automated compliance requirements into its systems to permit monitoring and auditing of its activities, as well as providing one level of proof of that compliance.

CSEC's policies and procedures for retention and disposal of acquired communications provide sufficient direction to CSEC employees respecting these activities and the protection of the privacy of Canadians. The retention and disposal periods set out in CSEC policies are reasonable. However, CSEC's inconsistent use of certain terminology in foreign signals intelligence and IT security policies is confusing and should be clarified. I will monitor CSEC efforts to clarify these policies.

I also found that CSEC had implemented recommendations made by my predecessors to establish records management authorities and retention and disposition schedules.

Conclusion

I concluded that CSEC conducted its retention and disposal activities during the period under review in accordance with legal and ministerial requirements and its policies and procedures.

2. CSEC's operations centre and particular foreign signals intelligence collection activities conducted in 2010

Background

CSEC's operations centre serves as the primary point through which CSEC interacts with Government of Canada clients, international partners and various internal CSEC sections during times of significantly elevated or unexpected activity. During such periods, the centre provides increased coordination. As part of its routine duties, the centre coordinates and produces a daily operational brief for the Chief of CSEC and provides other information to management, as required.

Findings

My review focused on an examination of the centre through an assessment of some of its activities conducted in 2010 under CSEC's mandates for foreign signals intelligence collection and assistance to federal law enforcement and security agencies. My highest priority was to assess the potential for risk posed to privacy in the conduct of these activities.

I also paid particular attention to CSEC's processing of requests from Government of Canada clients for releases of Canadian identity information suppressed in foreign signals intelligence reports produced by the centre. CSEC conducted these activities appropriately.

In novel or uncertain circumstances characteristic of an operations centre, I found that CSEC's use of temporary policy instruments to streamline approval processes in particular situations was appropriate. More broadly, CSEC managers and employees were aware of all relevant policies and procedures. CSEC managers routinely monitored their teams' activities to ensure compliance with both law and policy.

However, CSEC's operational instructions for some activities provided only limited direction specific to the nature of the operations centre. CSEC recognized this gap and is developing an operational instruction tailored to the centre's activities. I will monitor the implementation of this solution.

Conclusion

I concluded that CSEC conducted the examined activities in accordance with the law and ministerial requirements. A primary factor affecting my decision to review CSEC's operations centre was the potential for error in situations of increased pressure and time constraints. I found that, despite these circumstances in which the centre operated, the activities examined did not present any greater risk to compliance or to the privacy of Canadians than activities conducted by other sections of CSEC during routine business.

3. Update on an ongoing review of CSEC's foreign signals intelligence sharing with international partners

Background

It is common knowledge that Canada is a net importer of intelligence. CSEC's ability to fulfill its foreign signals intelligence collection and IT security mandates rests, in part, on building and maintaining productive relations with its foreign counterparts. CSEC's long-standing relationships with its closest allies — the United States' National Security Agency, the United Kingdom's Government Communications Headquarters, the Australian Defence Signals Directorate, and the New Zealand Government Communications Security Bureau — continues to benefit CSEC, and, in turn, the Government of Canada. This cooperative alliance may be more valuable now than at any other time, in the context of increasingly complex technological challenges.

The global nature of terrorism requires security and intelligence agencies to cooperate and share information with one another. The Government of Canada's response to the Report of the Standing Committee on Public Safety and National Security *Review of the Findings and Recommendations Arising From the Iacobucci and O'Connor Inquiries*, recognized that:

> the exchange of information with foreign partners raises unique challenges — policy, legal and operational — that are examined

> on a case-by-case basis in the context of Canada's national security environment. The cumulative result of successive commissions of inquiry, reports and lessons learned has been the refinement of policies and practices surrounding the exchange of information between foreign partners and Canada's national security and intelligence and law enforcement communities. (p. 4)

The need for information sharing is vital. However, information must be exchanged in compliance with the laws of Canada and must include sufficient measures to protect the privacy of Canadians. Although these cooperative arrangements include a commitment by the partners to respect the privacy of each others' citizens, it is recognized each partner is an agency of a sovereign nation that may derogate from the agreements, if it is judged necessary for their respective national interests.

Past Commissioners have also examined specific aspects of CSEC's foreign signals intelligence collection cooperation and sharing with international partners. This year, as part of this focused review, I provided the Minister with an update on my ongoing review of these activities.

Findings

Thus far, I have found that CSEC does take measures to protect the privacy of Canadians in what it shares with its international partners. For example, CSEC suppresses Canadian identity information in what is shared with its international partners. In addition, open and ongoing communications among the partners helps to limit the potential to affect the privacy of a Canadian.

However, my review has also identified some important questions that I will continue to examine in the coming year, including: how does CSEC assure itself that its international partners follow the long-standing agreements and practices that provide a foundation for CSEC's foreign signals intelligence information sharing?

I will complete my review in 2012–2013.

4. Annual combined review of CSEC foreign signals intelligence ministerial authorizations

Background

Subsection 273.65(8) of the *National Defence Act* requires me to review CSEC activities carried out under ministerial authorizations "to ensure they are authorized and report annually to the Minister [of National Defence] on the review". An annual combined review of the foreign signals intelligence collection ministerial authorizations is one way that I fulfill this part of my mandate. This year, I examined the five foreign signals intelligence ministerial authorizations in effect in 2009–2010 relating to five activities or class of activities. The purpose of this annual combined review of the five foreign signals intelligence collection ministerial authorizations is to:

1. identify any significant changes to the ministerial authorization documents themselves or to CSEC's activities described in the authorizations;

2. assess the impact, if any, of these changes on the risk of non-compliance and on the risk to privacy, and, as a result, identify any subjects requiring follow-up review; and

3. examine a sample of my choosing of any resulting private communications unintentionally intercepted by CSEC during the conduct of the activities under the ministerial authorizations.

Findings

Within this approach, I assessed whether CSEC's foreign signals intelligence collection activities complied with the law and protected the privacy of Canadians. I found that the activities carried out by CSEC under these ministerial authorizations were authorized. I also reviewed a sample of private communications retained by CSEC but that were not used in CSEC reports. I found that CSEC retained only those private communications essential to international affairs, defence or security, as required by paragraph 273.65(2)(*d*) of the *National Defence Act*.

For each of the five foreign signals intelligence collection activities, I examined certain key information relating to interception and to the privacy of Canadians, to permit comparison of the activities and to identify any significant changes or trends over time.

The 2009–2010 foreign signals intelligence collection ministerial authorizations did not contain any significant changes from the previous year and CSEC did not make any significant changes to the technologies used for these activities. CSEC did, however, clarify and enhance associated operational policies, including direction relating to the protection of the privacy of Canadians.

In addition, the effective periods for the ministerial authorizations changed — starting and ending on different dates from previous years' authorizations. This affected my ability this year to examine year-to-year changes in certain metrics relating to interception and to the privacy of Canadians. In addition, certain information on intercepted communications involving CSEC's international partners was not readily available. I will examine this issue as part of my ongoing review of CSEC's foreign signals intelligence information-sharing activities with these partners.

I examined CSEC's activities in response to a 2009 recommendation that CSEC establish formal management processes for when CSEC considers undertaking certain proposed foreign signals intelligence collection activities and for the recording of the resulting decision. I found that CSEC addressed this recommendation in an amendment to an operational policy.

As of the end of the 2011–2012 reporting period, I am awaiting a response from the Minister of National Defence to a recommendation I made in last year's report that CSEC be required, in a ministerial authorization, to report to the Minister certain information relating to privacy. This requirement would support the Minister in his accountability for CSEC, including for the measures CSEC takes to protect the privacy of Canadians. The Minister had initially supported CSEC's rejection of this recommendation. However, I sent the Minister

further information and I understand that CSEC is now reviewing this matter. I remain of the view that CSEC should implement this recommendation.

CSEC implemented a compliance validation program for its foreign signals intelligence activities. Changes to associated operational policy are also under development to address a recommendation in my review last year on this subject, as well as in response to a related audit report by CSEC's internal auditors. Next year, I will begin a detailed review of CSEC's management control framework and how this program helps CSEC document and demonstrate compliance with legal and policy obligations.

Conclusion

Apart from the instance on maintaining a recommendation from 2010–2011, my review contained no recommendations.

5. Annual review of a sample of disclosures of Canadian identity information to Government of Canada clients for calendar year 2011

Background

My predecessor directed in 2010 that an annual review of a sample of disclosures of Canadian identity information to Government of Canada clients be conducted, to verify that CSEC continues to comply with the law and maintains measures to protect the privacy of Canadians.

Canadian identity information may be included in CSEC's foreign signals intelligence reports if it is required to understand or use foreign intelligence. However, any information that identifies a Canadian must be suppressed in the reports — that is, replaced by a generic reference such as "a named Canadian". When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC must verify that the requesting client has both the authority and operational justification for obtaining the Canadian identity information. Only then may CSEC provide that information.

Findings

I examined a sample representing approximately 20 percent of the total number of requests approved during the period under review. The sample included disclosures made to all of the Government of Canada departments and agencies that had requested Canadian identity information during the period under review. My officials examined: the requests documenting the clients' authority and justification for obtaining the Canadian identity information; associated CSEC foreign signals intelligence reports; and the actual disclosures of Canadian identity information.

I found that CSEC's disclosure of suppressed Canadian identity information to Government of Canada clients was conducted in compliance with the law. Operational policies and procedures are in place and provide sufficient direction to CSEC employees respecting the protection of the privacy of Canadians and CSEC employees were knowledgeable about, and acted in accordance with, the policies and procedures.

I also examined CSEC's progress since last year to address my 2010 recommendations relating to tools that could support the tracking of disclosures of Canadian identity information and improve the consistency and accuracy of related reporting. CSEC provided my officials with a demonstration of the capabilities of a new system for disclosures that has been introduced and will address the recommendations. I will continue to monitor the implementation of this system, and will ensure that it sufficiently incorporates safeguards to protect the privacy of Canadians.

Conclusion

My review did not result in any recommendations. However, my officials observed and communicated to CSEC that the section responsible for processing disclosure requests did not show its usual meticulousness during the period under review. Nevertheless, my officials found during their examination clear evidence that the activities were lawful and conducted in accordance with policies and procedures. While the gaps in CSEC's records did not lessen the protection of the

privacy of Canadians in respect of those disclosures, I alerted CSEC to these gaps for the purpose of eliminating them.

6. and 7. Annual review of incidents identified by CSEC in 2010 and annual review of incidents identified by CSEC in 2011 that affected or had the potential to affect the privacy of Canadians and the measures taken by CSEC to address them

Background

In 2007, the Chief of CSEC wrote to the Commissioner to inform him that CSEC had created a central file describing CSEC operational incidents that did or could impact the privacy of Canadians. The Chief indicated that the file would be made available to the Commissioner for review as a proactive means to demonstrate CSEC's commitment to protecting privacy, helping ensure transparency and enhancing public confidence in CSEC.

According to CSEC, it records in this central file any incidents that put at risk the privacy of a Canadian in a manner that runs counter to or is not provided for in its operational policies. CSEC policy requires CSEC foreign signals intelligence and IT security employees to report and document privacy incidents in order to demonstrate compliance with CSEC policies and legal requirements, and to prevent further incidents. Incidents could include the inadvertent inclusion of Canadian identity information in a report, or mistakenly sharing certain reports with the wrong recipient.

My reviews of CSEC activities include an examination of any privacy incidents relating to the subject under review. The objectives of such annual reviews are to: acquire knowledge of the incidents and of corrective actions; and inform development of my work plan, by determining if there are any systemic issues or issues about compliance with the law or the protection of the privacy of Canadians that should be

subject to follow-up review. The review of these privacy incidents identified by CSEC also assists me in evaluating CSEC's management control framework. My employees are vigilant during other reviews about identifying this type of error, so we can confirm whether CSEC also identified and addressed them.

2010 findings

In early 2011, I conducted an initial review of all of the 2010 privacy incidents in CSEC's central file, but did not complete the review in time to report last year. I examined all foreign signals intelligence and IT security privacy incidents and the subsequent actions taken by CSEC to correct the incidents, focusing on those incidents not examined in detail in my other reviews.

I was satisfied that CSEC took appropriate corrective actions in a timely manner in response to the privacy incidents it recorded during 2010. My review did not reveal any systemic deficiencies or issues that required follow-up review. I also noted that CSEC revised guidance about how to respond to certain privacy incidents.

2010 conclusion

My review of the privacy incidents in 2010 did not result in any recommendations. However, my officials identified and communicated to CSEC suggestions to make CSEC's central file complete and consistent, in particular concerning the assessment of potential consequences flowing from the privacy incidents, and verifying whether and when corrective actions had been taken.

2011 findings

In 2012, I examined all foreign signals intelligence and IT security privacy incidents recorded by CSEC in calendar year 2011, and the subsequent actions taken by CSEC to correct the incidents.

I was particularly interested in the remedial actions CSEC plans to take to address three particular privacy incidents. One involved CSEC issuing guidance to address a policy gap relating to CSEC exchanges of information containing Canadian identity information. This gap was

identified during one of my ongoing reviews. For two other privacy incidents relating to certain IT security activities, I am also pleased to note that CSEC will issue guidance for handling certain information and associated reporting. I will monitor CSEC's efforts to address these follow-on activities.

2011 conclusion

I am satisfied that CSEC took appropriate corrective actions in response to the privacy incidents it recorded in 2011. My review of the privacy incidents in 2011 did not reveal any systemic deficiencies or issues that require follow-up review. I did not make any recommendations.

I was generally satisfied that CSEC addressed the suggestions I made about it's central file in 2010 to make it complete and consistent. Most entries for 2011 contained sufficient information, including corrective and mitigation actions taken by CSEC or by its partner agencies.

COMPLAINTS ABOUT CSEC'S ACTIVITIES

In 2011–2012, I received no complaints about CSEC activities that warranted investigation. This is not surprising because CSEC directs its activities at foreign entities located outside Canada.

For details on the complaints process, visit the CSE Commissioner's website (www.ocsec-bccst.gc.ca).

DUTY UNDER THE *SECURITY OF INFORMATION ACT*

I have a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy seeking to defend the release of special operational information — such as certain information relating to CSEC's activities — on the grounds that it is in the public interest.

No such matters were reported to me in 2011–2012.

ACTIVITIES OF THE COMMISSIONER'S OFFICE

Review Agencies Forum

The Review Agencies Forum comprises officials from my office, the Security and Intelligence Review Committee (SIRC), the Office of the Inspector General of the Canadian Security Intelligence Service, the Commission for Public Complaints Against the Royal Canadian Mounted Police, and the Office of the Privacy Commissioner. The Forum contributes to the development of the review community through the exchange of expertise, research, developments in legislation and case law, and best practices relating to review. This year, a senior manager from the Security and Intelligence Secretariat of the Privy Council Office met with the Forum to discuss the government's national security priorities and developments as well as proposals to strengthen review agencies and address the findings of recent inquiries.

My office also delivered a second review workshop to provide formalized training to staff from Forum organizations that are relatively new to the function of review.

Code of Values, Ethics and Conduct

I approved a Code of Values, Ethics and Conduct that applies to all individuals employed by my office. The Code contains specific responsibilities and expected behaviours of employees relating to the conduct of their work and reviews of CSEC. This Code fulfills the requirement of section 5 of the *Public Servants Disclosure Protection Act*. I am confident that commitment to these values and observance of the Code's behaviours will strengthen the ethical culture of the Commissioner's office and contribute to its integrity.

Other activities

In September, my office's Executive Director met with a Brazilian Federal Prosecutor who was a visiting academic at the Canadian Centre for Intelligence and Security Studies of Carleton University. This meeting informed the prosecutor's work on accountability and review mechanisms for Brazilian intelligence activities.

In October, my office's Executive Director, Director of Operations and legal counsel joined me at the Canadian Institute for the Administration of Justice's conference, *Terrorism, Law and Democracy: 10 years after 9/11*. Leading experts on national security law, privacy and related topics explored how changes to Canadian law to combat terrorism have affected fundamental rights and values of procedural justice in the last decade. Together with the former Independent Reviewer of Terrorism Legislation in the United Kingdom and the former Chair of SIRC, I participated in a panel on procedure and accountability in anti-terrorism matters. We discussed the role and importance of independent review of security and intelligence agencies in the Canadian and international contexts.

Also in October, officials from my office participated in a conference on the integration of privacy rights into security technologies, *Vers une intégration du droit à la vie privée et des technologies de sécurité*. The conference was organized by the *Centre de recherche en droit public* of the University of Montréal. My Executive Director participated in a panel and provided his perspectives on distinctions between national security and public safety and the integration of technology and privacy protection in national security. This conference also afforded my employees an opportunity to meet with Canadian and international civil servants, academics and students interested in issues of privacy, national security and public safety.

In November, my employees and I attended the annual international conference of the Canadian Association for Security and Intelligence Studies (CASIS) in Ottawa. For the past 10 years, my office has supported CASIS conferences and seminars offered to members and students interested in broadening understanding of the issues affecting security and intelligence. Under this year's theme, *New Frontiers in Security and Intelligence*, the conference explored new developments in this field.

The activities of CSIS are subject to review by SIRC. Those of CSEC are subject to review by me. SIRC and my own office are two separate, distinct and autonomous entities. SIRC may not investigate CSEC activities. My office may not investigate CSIS activities. It follows that when CSEC is acting at the request of CSIS, my powers of review begin only at the moment the request is made and are confined to the activities of CSEC — from the time the request is made, to the delivery of any information to CSIS. This year, I initiated discussions with the Chair and members of SIRC, and my Executive Director forwarded to SIRC a discussion paper on proposals for varying levels of cooperation in the conduct of reviews of activities involving both CSEC and CSIS. As I noted in my introduction, there is opportunity, under existing authorities, for greater collaboration between SIRC and my office, to enhance the effectiveness of review, in the spirit of the recommendations of the commission of inquiry led by the Honourable Justice Dennis O'Connor. In the coming year, I will pursue discussion of proposals to enhance collaboration of reviews of joint CSEC-CSIS activities.

CSEC is a highly technical organization, and my office is expected to keep pace with the rapid technological changes affecting CSEC's activities. For this reason, CSEC includes my employees in CSEC training, including introductory courses CSEC provides to new employees and training for the use of specific systems and databases.

WORK PLAN — REVIEWS UNDER WAY AND PLANNED

The results of several reviews currently underway are expected to be reported to the Minister of National Defence in the coming year and will be included in my 2012–2013 annual report.

The subjects of these reviews include: CSEC's foreign signals intelligence sharing with international partners; assistance to CSIS under CSEC's mandate to provide support to federal law enforcement and security agencies and sections 12 and 21 of the *CSIS Act*; and CSEC IT security activities conducted in support of Government of Canada departments' authorities under the *Criminal Code* and the *Financial Administration Act*.

Other reviews planned for 2012–2013, which may carry over to the next year, include reviews of: CSEC's Office of Counter-Terrorism and its activities and interactions with CSIS; particular signals intelligence collection activities conducted under ministerial authorizations; IT security activities conducted under ministerial authorizations; and CSEC's management control framework and compliance monitoring activities.

In addition, I will continue the annual reviews of foreign signals intelligence ministerial authorizations, CSEC disclosures of Canadian identity information to government clients, and privacy incidents identified by CSEC and the measures subsequently taken by CSEC to address them.

THE UPCOMING YEAR

The coming year promises to be eventful.

In May 2012, Canada hosts the 8th International Intelligence Review Agencies Conference in Ottawa. This is the second time that Canada is hosting this biennial conference, created in 1997. This year, it will bring together representatives of review bodies from 10 countries.

This Conference constitutes a unique opportunity for all of us to each share our experiences with the others and to gain from drawing comparisons. When it comes to review, there is no standard structure. Some countries stress the role of Parliamentarians, others that of independent review bodies headed by appointed officials. Canada will use this opportunity to report on changes since we last hosted the Conference in 1999. This retrospective over the past thirteen years should give us the necessary perspective to better assess today's reality and better predict tomorrow's.

This opportunity for perspective comes at the right time. The studies undertaken in Canada in recent years, particularly in the wake of the recommendations of Commissioners O'Connor, Iacobucci and Major on the possible reorganization of the intelligence and security review community, should bear fruit before long. Will some organizations be

shut down? — or merged? — or a new one created? — or a super-organization set up? Will there be a role for Parliamentarians and, if so, what kind? These are all questions that will give rise to a promising debate to which I look forward to contributing.

I must raise once again the matter of clarifying certain provisions of the *National Defence Act*, something my predecessors and I have proposed repeatedly. I concede that this is a matter of opportunity and political context. But I confess to being deeply disappointed at the time that has passed without addressing the ambiguities in the Act which, to my mind, should raise no controversy.

Finally, the title I have been given, Commissioner of the Communications Security Establishment, gives the impression that I am part of CSEC, whereas, on the contrary and for the reasons that led to my position being created in the first place, I am entirely independent. I have asked that this unfortunate designation be corrected.

ANNEX A: EXCERPTS FROM THE *NATIONAL DEFENCE ACT AND THE SECURITY OF INFORMATION ACT* RELATED TO THE MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

***National Defence Act* – Part V.1**

Appointment of Commissioner

273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

Duties

(2) The duties of the Commissioner are:

(*a*) to review the activities of the Establishment to ensure that they are in compliance with the law;

(*b*) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(*c*) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

Annual report

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

Powers of investigation

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the Inquiries Act.

Employment of legal counsel, advisors, etc.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

Directions

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

Transitional

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

[...]

Review of authorizations

273.65 (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

Security of Information Act

Public interest defence

15. (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]

Prior disclosure to authorities necessary

(5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]

(b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

ANNEX B: HISTORY OF THE OFFICE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

The Office of the Communications Security Establishment Commissioner was created on June 19, 1996, with the appointment of the inaugural Commissioner, the Honourable Claude Bisson, O.C., a former Chief Justice of Québec, who held the position until June 2003. He was succeeded by the late Right Honourable Antonio Lamer, P.C., C.C., C.D., LL.D., D.U., former Chief Justice of Canada, for a term of three years. The Honourable Charles D. Gonthier, C.C., Q.C., who retired as Justice of the Supreme Court of Canada in 2003, was appointed as Commissioner in August 2006, a position he held until his death in July 2009. The Honourable Peter deC. Cory, C.C., C.D., also a former Justice of the Supreme Court of Canada, served as Commissioner from December 14, 2009, to March 31, 2010. On June 18, 2010, the Honourable Robert Décary, Q.C., a former Justice of the Federal Court of Appeal, was appointed Commissioner.

For the first six years (from June 1996 to December 2001), the Commissioner carried out his duties under the authority of Orders in Council issued pursuant to Part II of the *Inquiries Act.* During this period, the Commissioner's responsibilities were twofold: to review the activities of the Communications Security Establishment Canada (CSEC) to determine whether they conformed with the laws of Canada; and to receive complaints about CSEC's activities.

The omnibus *Anti-terrorism Act,* which came into force on December 24, 2001, introduced amendments to the *National Defence Act* by adding Part V.1 and creating legislative frameworks for both the Commissioner's office and CSEC. It gave the Commissioner new responsibilities to review activities carried out by CSEC under a ministerial authorization. The legislation also continued the Commissioner's powers under the *Inquiries Act*.

The omnibus legislation also introduced the *Security of Information Act*, which replaced the *Official Secrets Act.* This legislation gives the Commissioner specific duties in the event that a person, who would otherwise be permanently bound to secrecy, seeks to defend the release of classified information about CSEC on the grounds that it is in the public interest.

While the Commissioner continues to provide the Minister of National Defence with his reports, the Commissioner's office is separate from, and not part of, the Department of National Defence.

ANNEX C: EXCERPTS FROM THE *NATIONAL DEFENCE ACT* RELATED TO THE MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT

The Communications Security Establishment Canada (CSEC) is Canada's national cryptologic agency, providing the Government of Canada with two key services: foreign signals intelligence, and information technology security. CSEC also provides technical and operational assistance to federal law enforcement and security agencies.

CSEC's foreign signals intelligence products and services support government decision-making in the fields of national security, national defence and foreign policy. CSEC's signals intelligence activities relate exclusively to foreign intelligence and are directed by the Government of Canada's intelligence priorities.

CSEC's information technology security products and services enable government departments and agencies to secure their electronic information systems and networks. CSEC also conducts research and development on behalf of the Government of Canada in fields related to communications security.

CSEC's three-part mandate is set out in subsection 273.64(1) of the *National Defence Act*:

> (*a*) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
>
> (*b*) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
>
> (*c*) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

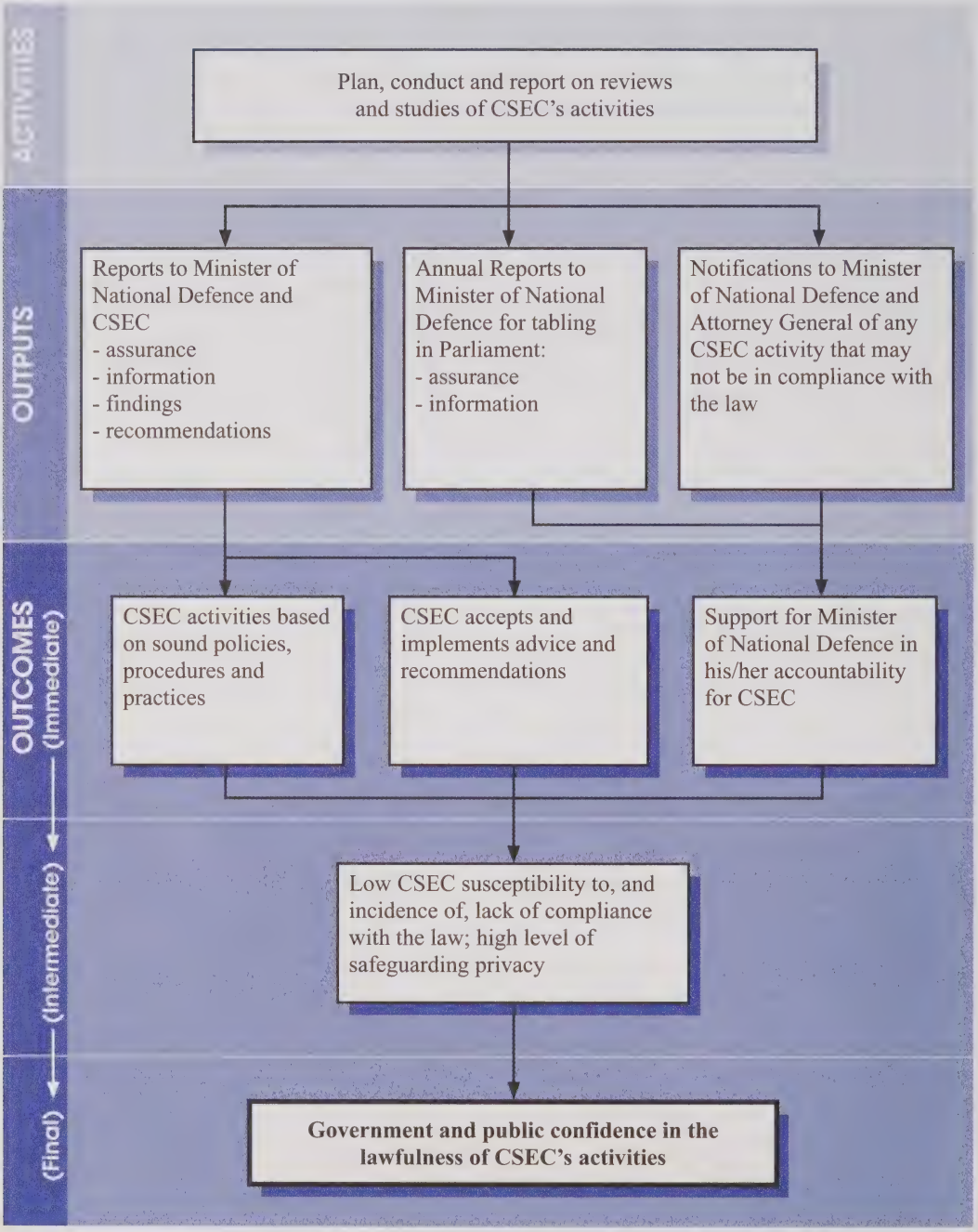
CSEC's website is: www.cse-cst.gc.ca.

ANNEX D: 2011-2012 STATEMENT OF EXPENDITURES

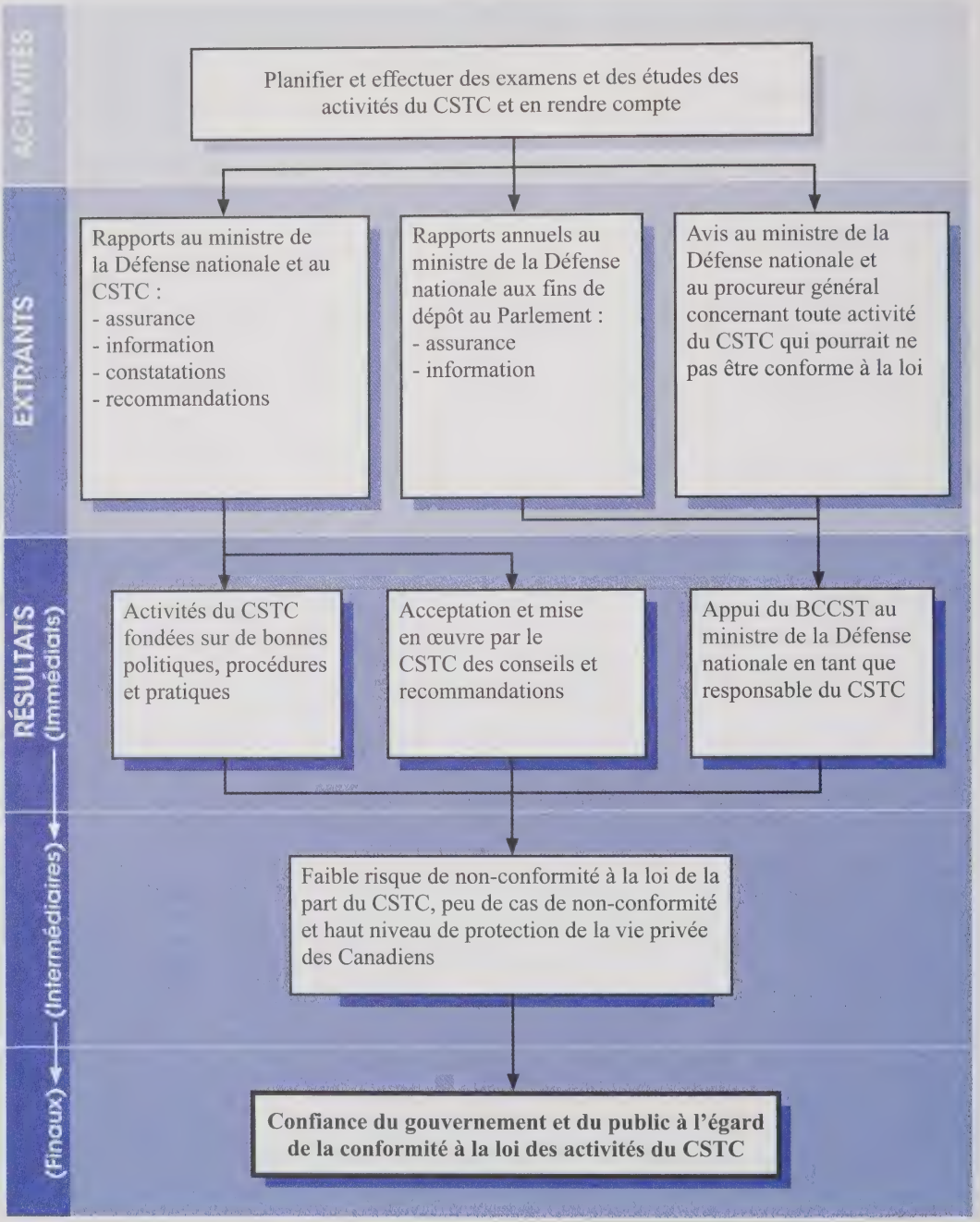
Standard Object Summary ($)

Salaries and Benefits		1,022,064
Transportation and Telecommunications		15,998
Information		11,652
Professional and Special Services		386,906
Rentals		168,110
Repairs and Maintenance		235
Material and Supplies		12,164
Machinery and Equipment		12,070
Assets		
Communications Equipment	29,759	
Office Equipment and Furniture	50,031	
Informatics Equipment	38,700	
Leasehold Improvements in Progress	194,740	
		313,230
Total		**1,942,429**

ANNEX E: COMMISSIONER'S OFFICE REVIEW PROGRAM — LOGIC MODEL



ANNEXE E : PROGRAMME D'EXAMEN DU BUREAU DU COMMISSAIRE – MODÈLE LOGIQUE



ANNEXE D : ÉTAT DES DÉPENSES 2011-2012

Sommaire des articles courants ($)

Traitements et salaires		1 022 064
Transport et télécommunications		15 998
Information		11 652
Services professionnels et spéciaux		386 906
Location		168 110
Réparations et entretien		235
Fournitures et approvisionnements		12 164
Machines et matériel		12 070
Actif		
Matériel de communication	29 759	
Matériel et ameublement de bureau	50 031	
Matériel informatique	38 700	
Améliorations locatives en cours	194 740	
		313 230
Total		**1 942 429**

ANNEXE C : EXTRAITS DE LA *LOI SUR LA DÉFENSE NATIONALE* SE RAPPORTANT AU MANDAT DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

Le CSTC est l'organisme national de cryptologie du pays qui offre au gouvernement du Canada deux services essentiels : il fournit des renseignements électromagnétiques étrangers et assure la sécurité des technologies de l'information. Le Centre offre en outre une assistance technique et opérationnelle aux organismes fédéraux chargés de la sécurité et de l'application de la loi.

Les produits et services de renseignement étranger du CSTC sont fournis à l'appui des décisions gouvernementales dans les domaines de la sécurité nationale, de la défense nationale et de la politique étrangère. Ses activités en matière de renseignements électromagnétiques visent exclusivement des renseignements étrangers et sont dictées par les priorités du gouvernement du Canada en matière de renseignement.

Dans le domaine de la sécurité des technologies de l'information, les produits et services du CSTC permettent aux ministères et organismes gouvernementaux d'assurer la sécurité de leurs systèmes et réseaux d'information électronique. Le CSTC effectue aussi des travaux de recherche-développement au nom du gouvernement du Canada dans des disciplines liées à la sécurité des télécommunications.

Le mandat à trois volets du CSTC est établi au paragraphe 273.64(1) de la partie V.1 de la *Loi sur la défense nationale* :

> *a*) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;
>
> *b*) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada; et
>
> *c*) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère.

Le site web du Centre est accessible à : (www.cse-cst.gc.ca).

ANNEXE B : HISTORIQUE DU BUREAU DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

Le Bureau du commissaire du Centre de la sécurité des télécommunications a été créé le 19 juin 1996, au moment de la nomination du premier commissaire, l'honorable Claude Bisson, O.C., ancien juge en chef du Québec qui a occupé le poste de commissaire jusqu'en juin 2003. Le très honorable Antonio Lamer, c.p., C.C., c.d., LL.D., d.u., ancien juge en chef du Canada, lui a succédé pour un mandat de trois ans. L'honorable Charles D. Gonthier, C.C., c.r., qui avait pris sa retraite de la Cour suprême du Canada en 2003, a été nommé commissaire en août 2006, et a occupé cette charge jusqu'à son décès en juillet 2009. L'honorable Peter deC. Cory, C.C., c.d., ancien juge de la Cour suprême du Canada, a occupé la charge de commissaire du 14 décembre 2009 au 31 mars 2010. Le 18 juin 2010, l'honorable Robert Décary, c.r., ancien juge de la Cour d'appel fédérale a été nommé commissaire.

Pendant les six premières années de son mandat (de juin 1996 à décembre 2001), le commissaire a exercé ses fonctions conformément à plusieurs décrets pris en vertu de la partie II de la *Loi sur les enquêtes*. Au cours de cette période, il a assumé une double responsabilité : examiner les activités du CSTC afin de déterminer si elles étaient en conformité avec les lois du Canada, et recevoir les plaintes relatives aux activités du CSTC.

La *Loi antiterroriste* omnibus, qui a été promulguée le 24 décembre 2001, a modifié la *Loi sur la défense nationale* en y ajoutant la partie V.1 et en créant le cadre législatif à la fois pour le Bureau du commissaire et pour le Centre. Elle confie au commissaire de nouvelles responsabilités relatives à l'examen des activités que mène le CSTC sous le régime d'une autorisation ministérielle et confirme également les pouvoirs du commissaire en vertu de la *Loi sur les enquêtes*.

La *Loi omnibus* a également introduit la *Loi sur la protection de l'information*, qui remplace la *Loi sur les secrets officiels*. La nouvelle loi attribue au commissaire des fonctions précises pour le cas où une personne astreinte au secret à perpétuité souhaiterait invoquer la défense de l'intérêt public pour justifier la divulgation de renseignements classifiés sur le CSTC.

Bien que le commissaire transmette toujours ses rapports au ministre de la Défense nationale, le Bureau est désormais un organisme distinct, qui ne fait plus partie de ce ministère.

Loi sur la protection de l'information

Défense d'intérêt public

15. (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public. [...]

Informer les autorités

(5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes : [...]

b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession, [...]

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable.

Pouvoirs d'enquête

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

Assistance

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

Fonctions du commissaire

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

Disposition transitoire

(7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.

[...]

Révision

273.65 (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.

ANNEXE A : EXTRAITS DE LA *LOI SUR LA DÉFENSE NATIONALE* ET DE LA *LOI SUR LA PROTECTION* DE L'INFORMATION SE RAPPORTANT AU MANDAT DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

Loi sur la défense nationale **– Partie V.1**

Nomination du commissaire

273.63 (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

Mandat

(2) Le commissaire a pour mandat :

a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées; and

c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

Rapport annuel

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

Ottawa. C'est la deuxième fois que le Canada est l'hôte de cette conférence biennale inaugurée en 1997. Elle regroupera cette année des représentants d'organismes de surveillance venant de dix pays.

Cette Conférence constitue une occasion unique pour nous tous de partager le fruit de nos expériences respectives et de tirer profit des comparaisons. Il n'y a pas de structure uniforme en matière de surveillance. Certains pays mettent l'accent sur le rôle des parlementaires; d'autres, sur le rôle d'organismes de surveillance indépendants ayant à leur tête des fonctionnaires nommés. Le Canada profitera de l'occasion pour faire état des changements survenus chez lui depuis qu'il a présidé la Conférence, en 1999. Ce regard sur les treize dernières années devrait nous donner le recul nécessaire pour mieux jauger la réalité d'aujourd'hui et mieux prévoir celle de demain.

Cette possibilité de recul arrive au bon moment. Les réflexions entreprises ces dernières années au Canada dans la foulée, notamment, des recommandations des commissaires O'Connor, Iacobucci et Major au sujet d'une réorganisation possible de la communauté de surveillance des organismes de la sécurité et du renseignement, devraient porter fruit sous peu. Y aura-t-il abolition d'organismes? Ou fusion? Ou la création d'un nouvel organisme? Ou l'établissement d'un super-organisme? Y aura-t-il un rôle dévolu aux parlementaires, et, si oui, quel sera ce rôle? Autant de questions qui soulèveront un débat prometteur auquel je compte bien contribuer.

Je ne pourrai m'empêcher de remettre à l'ordre du jour la clarification de certaines dispositions de la *Loi sur la défense nationale* que mes prédécesseurs et moi-même avons proposée. Je veux bien comprendre qu'il y ait là question d'opportunité et de contexte politique. Mais j'avoue être surpris du temps que l'on met à éliminer les ambiguïtés que nous avons identifiées dans la Loi et qui, à mon avis, ne devraient susciter aucune controverse.

Enfin, le titre sous lequel je suis désigné, « commissaire du Centre de la sécurité des télécommunications », donne à penser que je fais partie du Centre alors qu'au contraire et de par les raisons mêmes qui ont mené à la création de mon poste, j'en suis tout à fait indépendant. J'ai demandé qu'on corrige cette désignation malheureuse.

PLAN DE TRAVAIL – EXAMENS EN COURS ET PRÉVUS

Les résultats de plusieurs examens actuellement en cours devraient être communiqués au ministre de la Défense nationale au cours de l'exercice à venir et il en sera fait état dans mon rapport annuel 2012–2013.

Parmi les sujets retenus pour ces examens, mentionnons : le partage de renseignements électromagnétiques étrangers du Centre avec des partenaires étrangers; l'aide du Centre au SCRS en vertu de son mandat d'assistance aux organismes fédéraux d'application de la loi et de sécurité et des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité;* et les activités du Centre relatives à la sécurité des technologies de l'information menées à l'appui des autorisations conférées aux ministères fédéraux en vertu du *Code criminel* et de la *Loi sur la gestion des finances publiques.*

D'autres examens prévus en 2012-2013 pourraient être reportés à l'exercice suivant, notamment l'examen du Bureau de l'anti-terrorisme du Centre ainsi que de ses activités et interactions avec le SCRS; l'examen des activités de collecte de renseignements électromagnétiques particuliers menées en vertu d'autorisations ministérielles; l'examen des activités relatives à la sécurité des technologies de l'information menées en vertu d'autorisations ministérielles; et l'examen du cadre de contrôle de gestion du Centre et des mesures que prend le Centre pour s'assurer qu'il agit en conformité avec la loi, les exigences ministérielles et ses propres politiques et procédures.

En outre, je poursuivrai l'examen annuel des autorisations ministérielles visant les renseignements électromagnétiques étrangers, celui de la divulgation par le Centre d'information concernant l'identité de Canadiens à des clients du gouvernement et celui des incidents relatifs à la vie privée de Canadiens consignés par le Centre et des mesures qu'il a prises à leur égard.

L'ANNÉE À VENIR

L'année qui vient s'annonce fébrile.

En mai 2012, le Canada sera l'hôte de la 8e Conférence internationale des organismes de surveillance des agences de renseignement qui se tiendra à

En novembre, le personnel du Bureau et moi-même avons assisté au Colloque international annuel de l'Association canadienne pour les études de renseignement et de sécurité (ACERS) à Ottawa. Au cours des 10 dernières années, mon Bureau a appuyé les colloques et les séminaires de l'ACERS offerts aux membres et aux étudiants désireux d'élargir leur compréhension des questions ayant une incidence sur la sécurité et le renseignement. Sous le thème de cette année, *New Frontiers in Security and Intelligence*, le colloque explorait les nouveaux développements dans le domaine.

Les activités du SCRS sont assujetties à l'examen du Comité de surveillance et celles du Centre sont assujetties à mon examen. Le Comité de surveillance et mon propre Bureau sont tous deux des entités autonomes distinctes et séparées. Le Comité de surveillance ne peut faire enquête sur les activités du Centre et mon Bureau ne peut faire enquête sur les activités du SCRS. Il s'ensuit que lorsque le Centre agit à la demande du SCRS, mes pouvoirs d'examen commencent uniquement au moment où la demande est faite et portent exclusivement sur les activités du Centre — de la date de la demande à celle de la communication de toute l'information au SCRS. Cette année, j'ai amorcé des discussions avec le président et les membres du Comité de surveillance, et le directeur exécutif de mon Bureau a envoyé au Comité de surveillance un document de discussion faisant état de propositions en vue d'instaurer divers niveaux de coopération dans la conduite des examens des activités impliquant à la fois le Centre et le SCRS. Comme je l'ai mentionné dans mon introduction, il est possible de mettre en place une plus grande collaboration entre le Comité de surveillance et mon Bureau, sous le régime des autorisations actuelles, afin d'améliorer l'efficacité de l'examen, dans l'esprit des recommandations de la commission d'enquête dirigée par l'honorable juge Dennis O'Connor. Au cours de l'exercice à venir, je poursuivrai l'analyse de propositions pour renforcer la collaboration dans le cadre d'examens des activités menées conjointement par le CSTC et le SCRS.

Le Centre est une organisation hautement technique et mon Bureau doit être en mesure de s'adapter au rythme rapide des changements technologiques qui ont une incidence sur les activités du Centre. C'est pourquoi le Centre permet aux employés de mon Bureau de participer à la formation qu'il offre à l'interne, notamment aux cours d'introduction qui s'adressent aux nouveaux employés et à la formation pour l'utilisation de bases de données et de systèmes particuliers.

des fonctionnaires divulgateurs d'actes répréhensibles. Je suis convaincu que l'engagement des employés à l'égard de ces valeurs et leur adhésion aux comportements prescrits par le code renforceront la culture éthique du Bureau du commissaire et contribueront à son intégrité.

Autres activités

En septembre, le directeur exécutif du Bureau a rencontré un procureur général brésilien qui était un universitaire invité au Canadian Centre for Intelligence and Security Studies de l'Université Carleton. Cette rencontre a aidé le procureur dans son travail concernant les mécanismes de reddition de comptes et d'examen des activités du renseignement brésilien.

En octobre, le directeur exécutif, le directeur des opérations et la conseillère juridique de mon Bureau se sont joints à moi pour assister à la Conférence de l'Institut canadien d'administration de la justice intitulée *« Terrorisme, Droit et Démocratie : 10 ans après le 11 septembre 2001 »*. D'éminents experts en droit de la sécurité nationale, protection de la vie privée et autres sujets connexes ont exploré la façon dont les changements apportés à la législation canadienne pour combattre le terrorisme ont affecté les droits fondamentaux et les valeurs de la justice procédurale au cours de la dernière décennie. En compagnie de l'ancien observateur indépendant de la législation anti-terroriste du Royaume-Uni et de l'ancien président du Comité de surveillance, j'ai participé à un panel sur la procédure et la reddition de comptes en matière d'anti-terrorisme. Nous avons discuté du rôle et de l'importance de l'examen indépendant des organismes voués à la sécurité et au renseignement dans le contexte canadien et international.

En octobre également, des employés de mon Bureau ont participé à la conférence intitulée *Vers une intégration du droit à la vie privée et des technologies de sécurité* organisée par le Centre de recherche en droit public de l'Université de Montréal. Le directeur exécutif du Bureau a participé à un panel et présenté son point de vue sur les distinctions entre la sécurité nationale et la sécurité publique ainsi que sur l'intégration de la technologie et de la protection de la vie privée dans la sécurité nationale. Grâce à cette conférence, les employés de mon Bureau ont eu la possibilité de rencontrer des fonctionnaires, des universitaires et des étudiants canadiens et étrangers intéressés par les questions de vie privée, de sécurité nationale et de sécurité publique.

MANDAT SOUS LE RÉGIME DE LA *LOI SUR LA PROTECTION DE L'INFORMATION*

Je suis tenu, en vertu de la *Loi sur la protection de l'information*, de recevoir de l'information émanant de personnes astreintes au secret à perpétuité, qui ont l'intention de communiquer des renseignements opérationnels spéciaux — par exemple, certains renseignements se rapportant aux activités du Centre — en faisant valoir la primauté de l'intérêt public.

Aucune affaire de ce genre ne m'a été signalée en 2011-2012.

ACTIVITÉS DU BUREAU DU COMMISSAIRE

Forum des organismes de surveillance

Le Forum des organismes de surveillance réunit les représentants de mon Bureau, du Comité de surveillance, du Bureau de l'inspecteur général du SCRS, de la Commission des plaintes du public contre la Gendarmerie Royale du Canada et du Commissariat à la protection de la vie privée du Canada. Le Forum contribue au renforcement du milieu de la surveillance en favorisant l'échange d'expertise, de travaux de recherche, d'information sur tout développement législatif ou jurisprudentiel, et de modèles de pratique. Cette année, un cadre de haut niveau du Secrétariat de la sécurité et du renseignement du Bureau du Conseil Privé a rencontré les participants au Forum pour discuter des priorités du gouvernement et des développements en matière de sécurité nationale, de même que des propositions pour renforcer les organismes de surveillance et donner suite aux conclusions des récentes commissions d'enquête.

Mon Bureau a aussi offert un second atelier d'examen pour donner une formation structurée au personnel des organisations membres du Forum pour lequel la fonction d'examen est relativement nouvelle.

Code de valeurs, d'éthique et de conduite

J'ai approuvé un Code de valeurs, d'éthique et de conduite qui s'applique à tous les employés de mon Bureau. Le code fait état des responsabilités particulières et des comportements attendus des employés dans leurs activités professionnelles et dans la conduite des examens du Centre. Ce code répond à l'exigence énoncée à l'article 5 de la *Loi sur la protection*

Je me suis particulièrement intéressé aux mesures correctives que le Centre envisage de prendre relativement à trois incidents particuliers relatifs à la vie privée. Dans le premier cas, le Centre a émis des lignes directrices pour combler une lacune dans les politiques se rapportant aux échanges de renseignements contenant de l'information pouvant mener à l'identification de Canadiens. Cette lacune avait été mise en évidence à l'occasion de l'un de mes examens courants. En ce qui a trait aux deux autres incidents se rapportant à certaines activités relatives à la sécurité des technologies de l'information, je suis également heureux de signaler que le Centre émettra des lignes directrices visant le traitement et le rapport de certains renseignements. Je surveillerai les efforts du Centre pour concrétiser ces activités de suivi.

Conclusion pour 2011

Je suis convaincu que le Centre a pris des mesures correctives pertinentes en réponse aux incidents relatifs à la vie privée qu'il a consignés en 2011. Mon examen des incidents relatifs à la vie privée survenus en 2011 n'a pas mis au jour de lacunes ou de problèmes systémiques exigeant un suivi. Je n'ai pas formulé de recommandations.

Dans l'ensemble, je suis convaincu que le Centre a pris en compte les suggestions que je lui ai faites en 2010 concernant le dossier central pour rendre cohérent et exhaustif. La plupart des données saisies renfermaient suffisamment d'information, y compris les mesures correctives et d'atténuation prises par le Centre ou par les organismes qui sont ses partenaires.

PLAINTES CONCERNANT LES ACTIVITÉS DU CENTRE

En 2011-2012, je n'ai reçu aucune plainte justifiant une enquête. Cela n'est pas étonnant puisque les activités du Centre visent des entités étrangères situées à l'extérieur du Canada.

On trouvera des précisions sur le processus de plainte dans le site web du commissaire du Centre de la sécurité des télécommunications (www.ocsec-bccst.gc.ca).

L'examen de ces incidents relatifs à la vie privée signalés par le Centre m'a également aidé à évaluer son mécanisme de contrôle de gestion. Par ailleurs, les employés de mon Bureau font preuve de vigilance au cours d'autres examens de manière à détecter ce type d'erreurs, ce qui nous permet de vérifier si le Centre les a également détectées et corrigées.

Constatations pour 2010

Au début de 2011, j'ai effectué un examen initial de tous les incidents relatifs à la vie privée consignés en 2010 dans le dossier central du Centre, mais je ne l'ai pas complété à temps pour le rapport de l'an dernier. J'ai passé en revue tous les incidents liés aux renseignements électromagnétiques étrangers et à la sécurité des technologies de l'information susceptibles de porter atteinte à la vie privée ainsi que les mesures subséquentes prises par le Centre pour rectifier le tir, en mettant l'accent sur les incidents que je n'avais pas analysés en détail au cours de mes autres examens.

Je suis convaincu que le Centre a pris des mesures correctives appropriées en temps opportun par suite des incidents relatifs à la vie privée qu'il a consignés en 2010. Mon examen n'a pas révélé de lacunes ou de problèmes systémiques qui auraient exigé un suivi. J'ai également noté que le Centre avait révisé ses lignes directrices concernant la façon de répondre à certains incidents relatifs à la vie privée.

Conclusion pour 2010

Mon examen des incidents relatifs à la vie privée consignés en 2010 n'a pas entraîné de recommandations. Toutefois, les employés de mon Bureau ont formulé et communiqué au Centre des suggestions pour améliorer l'exhaustivité et la cohérence de son dossier central, en particulier en ce qui a trait à l'évaluation des conséquences pouvant découler des incidents relatifs à la vie privée, et à la vérification pour savoir si des mesures correctives ont été prises et quand elles l'ont été.

Constatations pour 2011

En 2012, j'ai examiné tous les incidents liés aux renseignements électromagnétiques étrangers et à la sécurité des technologies de l'information susceptibles de porter atteinte à la vie privée consignés au cours de l'année 2011, ainsi que les mesures prises par la suite pour corriger le problème.

aux procédures. Bien que les lacunes observées dans les dossiers du Centre relativement à ces divulgations n'aient pas amoindri la protection de la vie privée des Canadiens, j'ai avisé le Centre de combler ces lacunes.

6. et 7. Examen annuel des incidents signalés par le Centre en 2010 et 2011 qui ont touché ou auraient pu toucher la vie privée de Canadiens ainsi que des mesures prises par le Centre pour régler le problème

Contexte

En 2007, le chef a écrit au commissaire pour l'informer que le Centre avait créé un dossier central décrivant les incidents opérationnels internes qui avaient ou auraient pu toucher la vie privée de Canadiens. Le chef a indiqué que le dossier serait accessible au commissaire à des fins d'examen de manière à démontrer la détermination viscérale du Centre à protéger la vie privée, à faire preuve de transparence et à renforcer la confiance du public à son égard.

D'après le Centre, il consigne dans ce dossier central tout incident qui risque de porter atteinte à la vie privée d'un Canadien d'une manière qui n'est pas prévue dans ses politiques opérationnelles ou qui va à l'encontre de ces politiques. La politique du Centre exige que les employés qui travaillent sur les renseignements électromagnétiques étrangers et la sécurité des technologies de l'information signalent et documentent les incidents relatifs à la vie privée de façon à montrer la conformité aux politiques du Centre ainsi qu'à ses obligations en vertu de la loi et à prévenir d'autres incidents. Ces incidents pourraient comprendre l'intégration par inadvertance d'informations sur l'identité d'un Canadien dans un rapport du Centre ou le partage par erreur de certains rapports avec un destinataire qui n'était pas le destinataire visé.

Dans le cadre de mes examens, j'ai passé en revue tous les incidents relatifs à la vie privée se rapportant au sujet à l'étude. Ces examens annuels ont pour finalité de me faire prendre connaissance des incidents et des mesures correctives et de me guider dans l'élaboration de mon plan de travail en déterminant s'il y a des problèmes systémiques ou relatifs à la conformité à la loi ou à la protection de la vie privée des Canadiens qui devraient faire l'objet d'un examen de suivi.

d'une justification opérationnelle pour obtenir ce genre de renseignements. Ce n'est qu'une fois satisfait que le Centre fournit l'information.

Constatations

Mon examen a porté sur un échantillon d'environ 20 p. 100 du nombre total de demandes approuvées au cours de la période visée. L'échantillon comprenait des renseignements divulgués à tous les ministères et organismes du gouvernement du Canada qui avaient demandé et obtenu des informations sur l'identité de Canadiens au cours de la période. Des employés de mon Bureau ont examiné les documents présentés à l'appui des demandes ainsi que la justification présentée pour obtenir l'information sur l'identité de Canadiens. Ils ont aussi examiné les rapports pertinents du Centre sur les renseignements électromagnétiques étrangers ainsi que les renseignements effectivement divulgués sur l'identité de Canadiens.

Il appert que la divulgation par le Centre, aux clients du gouvernement du Canada, d'informations supprimées concernant l'identité de Canadiens a été faite conformément à la loi. Des politiques opérationnelles et des procédures sont en place pour fournir des consignes suffisantes aux employés du Centre concernant la protection de la vie privé des Canadiens. Les employés connaissaient bien les politiques et procédures en question et ont agi en conformité avec celles-ci.

Je me suis également penché sur les progrès réalisés par le Centre depuis l'an dernier dans la suite donnée à mes recommandations formulées en 2010 concernant les outils qui pourraient aider à assurer le suivi de la divulgation de renseignements sur l'identité de Canadiens et améliorer l'uniformité et l'exactitude des rapports connexes. Le Centre a présenté aux agents responsables de mon Bureau une démonstration des capacités d'un nouveau système pour les divulgations, qui a été mis en place et appliquera les recommandations. Je continuerai de surveiller la mise en œuvre de ce système et m'assurerai qu'il intègre suffisamment de garde-fous pour protéger la vie privée des Canadiens.

Conclusion

Aucune recommandation ne découle de mon examen, mais les employés de mon Bureau ont observé et indiqué au Centre que la section responsable du traitement des demandes de divulgation n'avait pas fait preuve de sa méticulosité habituelle au cours de la période à l'étude. Néanmoins, en approfondissant l'examen, ils ont trouvé des preuves témoignant clairement de la légalité des activités et de la conformité aux politiques et

et, à ma connaissance, le Centre réexamine actuellement cette question. Je demeure d'avis que le Centre devrait donner suite à cette recommandation.

Le Centre a mis en œuvre un programme de validation de conformité applicable à ses activités de collecte de renseignements électromagnétiques étrangers. Des changements à la politique opérationnelle connexe sont également en cours d'élaboration en vue de donner suite à une recommandation formulée au cours de mon examen effectué l'an dernier sur ce sujet, de même qu'en réponse à un rapport des vérificateurs internes du Centre à ce sujet. L'an prochain, j'entreprendrai un examen détaillé du mécanisme de contrôle de gestion mis sur pied par le Centre et de la façon dont ce programme aide le Centre à démontrer, documents à l'appui, comment il se conforme à la loi et à ses politiques.

Conclusion

Excepté le maintien d'une recommandation formulée en 2010-2011, mon examen ne renferme aucune recommandation.

5. Examen annuel d'un échantillon de renseignements concernant l'identité de Canadiens divulgués aux clients du gouvernement du Canada pour l'année 2011

Contexte

En ce qui a trait aux renseignements concernant l'identité de Canadiens divulgués au clients du gouvernement du Canada, mon prédécesseur avait décidé, en 2010, de procéder dorénavant à un examen annuel portant sur un échantillon pour vérifier si le Centre continue de se conformer à la loi et prend les mesures qui s'imposent pour protéger la vie privée des Canadiens.

Des rapports du Centre portant sur des renseignements électromagnétiques étrangers peuvent renfermer de l'information permettant d'identifier des citoyens canadiens si cette information est jugée essentielle à la compréhension ou à l'utilisation de ces renseignements. Cependant, toute information identifiant un Canadien doit être supprimée des rapports et remplacée par une mention générale du type « un Canadien ». Lorsqu'il reçoit une demande subséquente de divulgation de précisions sur l'information supprimée, le Centre doit vérifier que le client dont elle émane dispose à la fois de l'autorisation et

Concernant chacune des cinq activités de collecte de renseignements électromagnétiques étrangers, j'ai examiné certains renseignements clés se rapportant à l'interception et à la vie privée des Canadiens, ce qui me permettait de comparer les activités et de noter tout changement ou évolution d'importance.

Les autorisations ministérielles de 2009-2010 ne comportent aucun changement important par rapport à l'année précédente et le CSTC n'a pas non plus apporté de changements importants aux technologies utilisées pour ces activités. Le Centre a clarifié et amélioré ses politiques opérationnelles connexes, y compris les instructions se rapportant à la protection de la vie privée des Canadiens.

Par ailleurs, les périodes de validité des autorisations ministérielles ont changé: elles entrent en vigueur et expirent à des dates différentes des autorisations des années précédentes. Cet élément a affecté ma capacité à examiner cette année les variations d'une année à l'autre dans certaines données se rapportant à l'interception de communications et à la vie privée des Canadiens. En outre, certains renseignements sur les communications interceptées impliquant des partenaires étrangers du CSTC ne sont pas aisément accessibles. J'examinerai cette question dans le cadre de mon examen permanent des activités de partage des renseignements électromagnétiques étrangers du Centre avec ces partenaires.

J'ai examiné comment le Centre avait répondu à une recommandation de 2009 qui souhaitait qu'il établisse formellement des méthodes de gestion qu'il appliquerait au moment d'entreprendre certaines activités de collecte de renseignements électromagnétiques étrangers et au moment de consigner la décision qui en résulterait. J'ai observé que le Centre avait donné suite à cette recommandation en modifiant une politique opérationnelle.

À la fin de la période visée par ce rapport, j'attends la réponse du ministre de la Défense nationale à une recommandation que j'avais formulée dans mon dernier rapport à l'effet que le Centre soit tenu, dans les autorisations ministérielles, de faire rapport au ministre de certains renseignements se rapportant à la protection de la vie privée. Cette exigence appuierait le ministre dans l'exercice de sa responsabilité relativement au Centre, y compris concernant les mesures prises par ce dernier pour protéger la vie privée des Canadiens. Le ministre avait appuyé au départ le rejet de cette recommandation par le Centre. Toutefois, j'ai envoyé au ministre un complément d'information

4. Examen combiné annuel des autorisations ministérielles relatives aux renseignements électromagnétiques étrangers du Centre

Contexte

En vertu du paragraphe 273.65(8) de la *Loi sur la défense nationale,* je suis tenu de faire enquête sur les activités qui sont exercées sous le régime d'une autorisation ministérielle « pour en contrôler la conformité » et d'en rendre compte « annuellement au ministre [de la Défense nationale] ». L'une des façons de m'acquitter de ce volet de mon mandat consiste à effectuer un examen combiné annuel des autorisations ministérielles visant la collecte de renseignements électromagnétiques étrangers. Cette année, j'ai donc fait enquête sur les cinq autorisations ministérielles en vigueur en 2009-2010 se rapportant à cinq activités ou catégories d'activités. L'examen combiné annuel des cinq autorisations ministérielles vise trois objectifs :

1. Signaler tout changement d'importance dans le texte même des autorisations ou dans les activités du Centre décrites dans les autorisations;

2. Vérifier l'incidence, le cas échéant, de ces changements sur le risque de non-conformité et sur le risque d'atteinte à la vie privée et, en conséquence, cerner tout sujet nécessitant un examen de suivi; et

3. Examiner un échantillon de mon choix de toutes les communications privées interceptées fortuitement par le Centre au cours de la conduite de ses activités sous le régime d'une autorisation ministérielle.

Constatations

Selon cette méthode, j'ai évalué si les activités de collecte de renseignements électromagnétiques étrangers du Centre étaient conformes à la loi et protégeaient la vie privée des Canadiens. J'ai constaté que les activités menées par le Centre en vertu des autorisations ministérielles de 2009-2010 étaient dûment autorisées. J'ai également examiné un échantillon de communications privées conservées par le CSTC, mais non utilisées par ce dernier dans ses rapports. J'ai constaté que le CSTC ne conservait que les communications privées essentielles pour les affaires internationales, la défense ou la sécurité, comme l'exige l'alinéa 273.65(2)*d*) de la *Loi sur la défense nationale*.

> La communication de renseignements avec des partenaires étrangers soulève des défis particuliers sur les plans stratégique, juridique et opérationnel, et est examinée individuellement dans le cadre de l'environnement de la sécurité nationale du Canada. Les résultats cumulatifs des commissions d'enquête successives, des rapports et des leçons apprises ont mené à l'amélioration des politiques et des pratiques relatives à l'échange d'information entre les partenaires étrangers et les communautés canadiennes de la sécurité nationale, du renseignement et de l'application de la loi (p. 4).

Le partage de l'information est vital. Toutefois, les renseignements doivent être échangés en conformité avec les lois du Canada et des mesures suffisantes doivent être prévues pour protéger la vie privée des Canadiens. Même si ces ententes de coopération incluent un engagement des partenaires à respecter la vie privée de leurs citoyens respectifs, on sait pertinemment que chaque partenaire est un organisme d'un pays souverain qui peut déroger aux ententes s'il l'estime nécessaire pour les intérêts nationaux.

Les anciens commissaires se sont également penchés sur des aspects particuliers de la coopération en matière de collecte de renseignements électromagnétiques étrangers du Centre et des échanges avec des partenaires étrangers. Cette année, dans le cadre de cet examen ciblé sur le partage de renseignements électromagnétiques étrangers du CSTC, j'ai présenté au ministre une mise à jour de mon examen permanent de ces activités.

Constatations

À ce jour, il appert que le Centre prend des mesures pour protéger la vie privée des Canadiens dans ses échanges avec ses partenaires étrangers. Par exemple, le Centre supprime l'information relative à l'identité de Canadiens dans l'information qu'il partage avec ses partenaires étrangers. En outre, le fait que les partenaires communiquent fréquemment et ouvertement entre eux sur cette question aide à limiter le risque d'atteinte à la vie privée d'un Canadien.

Toutefois, mon examen a également mis en évidence certaines questions importantes que je continuerai d'approfondir au cours de l'année à venir, notamment : Comment le Centre s'assure-t-il que ses partenaires étrangers se conforment à des ententes et à des pratiques de longue date qui constituent le fondement du partage de renseignements électromagnétiques étrangers?

J'entends compléter mon examen en 2012-2013.

Conclusion

J'ai conclu que le CSTC avait mené les activités examinées conformément aux obligations en vertu de la loi et aux exigences ministérielles. Ma décision d'examiner le centre des opérations a été en grande partie motivée par le risque d'erreurs dans des situations de pression accrue et de contrainte de temps. J'ai constaté que, en dépit des conditions dans lesquelles le centre des opérations a exercé ses activités, les activités examinées n'ont pas présenté plus de risque au chapitre de la conformité ou de la vie privée des Canadiens que les activités menées par d'autres sections du CSTC au cours de leur travail routinier.

3. Mise à jour concernant l'examen en cours du partage des renseignements électromagnétiques étrangers du CSTC avec des partenaires étrangers

Contexte

Il est de notoriété publique que le Canada est un importateur net de renseignements. La capacité du CSTC à respecter ses mandats de collecte de renseignements électromagnétiques étrangers et de sécurité des technologies de l'information repose, en partie, sur l'établissement et le maintien de relations productives avec les organismes étrangers ayant la même vocation. La relation de longue date du CSTC avec ses plus proches alliés — la National Security Agency des États-Unis, le Government Communications Headquarters du Royaume-Uni, la Defence Signals Directorate de l'Australie et le Government Communications Security Bureau de la Nouvelle-Zélande — continue d'être avantageuse pour le CSTC et, en conséquence pour le gouvernement du Canada. Compte tenu de la complexité croissante des défis technologiques, cette alliance axée sur la coopération peut être plus précieuse que jamais auparavant.

En raison de la nature planétaire du terrorisme, les organismes voués à la sécurité et au renseignement n'ont d'autre choix que de coopérer et de partager l'information l'un avec l'autre. Dans sa réponse au Rapport du Comité permanent de la sécurité publique et nationale, intitulé *Examen des constats et recommandations émanant des enquêtes Iacobucci et O'Connor,* le gouvernement du Canada reconnaît que :

2. Activités du centre des opérations du CSTC et collecte de renseignements électromagnétiques étrangers particuliers menées en 2010

Contexte

Le centre des opérations du CSTC constitue le principal point d'interaction entre le CSTC et les clients du gouvernement du Canada, ses partenaires internationaux et certaines de ses sections internes au cours de périodes d'activité intense ou inattendue. Au cours de ces périodes, le centre des opérations assure une coordination accrue. Une de ses tâches de routine est de préparer un document opérationnel quotidien à l'intention du chef du CSTC et de fournir d'autres renseignements à la direction, au besoin.

Constatations

Mon examen a mis l'accent sur une évaluation de certaines des activités du centre d'opérations menées en 2010 en vertu des mandats de collecte de renseignements électromagnétiques étrangers et d'assistance aux organismes fédéraux chargés de la sécurité et de l'application de la loi. Ma grande priorité était d'évaluer le risque éventuel que représente la conduite de ces activités.

J'ai porté une attention particulière à la façon dont le CSTC a traité les demandes émanant de clients du gouvernement du Canada relatives à la divulgation d'information sur l'identité de Canadiens qui avait été supprimée des rapports produits par le centre des opérations. Le CSTC a conduit ces activités de façon appropriée.

Dans les circonstances nouvelles ou incertaines qui sont propres à un centre des opérations, j'ai constaté que l'utilisation par le CSTC d'instruments de politique temporaires pour simplifier les processus d'approbation dans des situations particulières était appropriée. De façon générale, les gestionnaires et les employés du CSTC étaient au courant de toutes les politiques et procédures pertinentes. Les gestionnaires du CSTC ont surveillé de façon routinière les activités de leurs équipes pour assurer la conformité tant à la loi qu'à la politique.

Toutefois, les instructions opérationnelles du CSTC ne pouvaient être appliquées que de manière limitée au centre des opérations, vu la nature des activités de ce dernier. Le CSTC a reconnu cette lacune et il est en voie d'élaborer une instruction opérationnelle adaptée aux activités du centre des opérations. Je surveillerai la mise en œuvre de cette solution.

lesquels le Centre peut rendre compte de ses activités et fournir l'assurance qu'elles sont conformes à ses obligations en vertu de la loi ainsi qu'aux exigences ministérielles et stratégiques. Mes prédécesseurs ont formulé plusieurs recommandations qui ont été à l'origine d'importants changements dans les pratiques de gestion de l'information du Centre et les systèmes connexes et qui ont eu pour effet de renforcer la conformité.

Constatations

J'ai constaté que tant le programme de collecte de renseignements électromagnétiques étrangers que le programme de sécurité des technologies de l'information du Centre ont intégré dans leur architecture numérique respective plusieurs moyens de satisfaire les obligations légales, les exigences ministérielles et les politiques du Centre relatives à la conservation et la destruction. J'ai acquis une connaissance détaillée et documentée de cette approche dictée à la fois par les politiques du Centre et par la technologie. Au cours de l'examen, j'ai constaté que le Centre avait intégré dans ses systèmes plusieurs exigences automatisées liées à la conformité qui permettent la surveillance et la vérification de ses activités et qui fournissent une certaine preuve de cette conformité.

J'ai également constaté que les politiques et les procédures adoptées par le Centre permettent à ses employés de bien mener leurs activités et de veiller à la protection de la vie privée des Canadiens. Les périodes de conservation et de destruction établies dans les politiques du Centre sont raisonnables. Toutefois, l'utilisation inconsistante par le Centre d'une certaine terminologie dans ses politiques porte à confusion et devrait être corrigée. Je surveillerai les efforts déployés par le CSTC pour clarifier ces politiques.

J'ai constaté que le Centre avait mis en œuvre les recommandations de mes prédécesseurs à l'effet d'établir les autorités de gestion des dossiers ainsi que les calendriers de conservation et de destruction.

Conclusion

J'ai conclu que le Centre avait mené ses activités de conservation et de destruction au cours de la période visée par l'examen en conformité avec ses obligations légales, les exigences ministérielles et ses politiques et procédures.

FAITS SAILLANTS DES SEPT RAPPORTS PRÉSENTÉS AU MINISTRE EN 2011-2012

1. Conservation et destruction par le CSTC des communications interceptées ou copiées

Contexte

La quantité croissante d'information électronique générée dans notre monde interconnecté complique la tâche du CSTC qui doit gérer la conservation (stockage) et la destruction des renseignements qu'il acquiert. Les programmes de collecte de renseignements électromagnétiques étrangers et de sécurité des technologies de l'information du Centre ont introduit récemment d'importants changements technologiques qui ont une incidence sur leurs pratiques de conservation et de destruction des communications acquises.

En vertu de l'alinéa 273.64(2)*b*) de la *Loi sur la défense nationale,* le Centre est tenu de prendre des mesures pour protéger la vie privée des Canadiens. Ces mesures visent la manière dont il conserve et détruit les communications qu'il intercepte au cours de ses activités de collecte de renseignements électromagnétiques étrangers ou de sécurité des technologies de l'information. Dans cet examen, j'ai accordé une attention particulière à la conservation et à la destruction des communications privées interceptées fortuitement et des renseignements sur l'identité de Canadiens.

En tant qu'institution fédérale, le Centre a par ailleurs l'obligation légale de conserver certains dossiers. La *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels* reconnaissent que les citoyens ont, dans des conditions bien précises, droit d'accès aux dossiers gouvernementaux. Des institutions fédérales comme le CSTC doivent également protéger tous les renseignements personnels qu'ils peuvent recueillir ou transmettre. Ces obligations en vertu de la loi renforcent l'obligation du CSTC de tenir un inventaire complet et détaillé donnant une description de l'information qu'il détient. En effet, la destruction sans autorisation d'un dossier pourrait entraîner l'incapacité de documenter une activité et, en conséquence, l'incapacité de faire la preuve de la conformité.

Mes prédécesseurs et moi-même avons toujours surveillé les pratiques de gestion de l'information du Centre étant donné que la création et la conservation des dossiers constitue l'un des principaux moyens par

APERÇU DES CONSTATATIONS DE 2011-2012

Au cours de l'exercice 2011-2012 visé par le rapport, j'ai présenté au ministre de la Défense nationale sept rapports portant sur mes examens des activités du Centre.

Ces examens ont été réalisés en vertu de deux volets de mon mandat :

- m'assurer que les activités du CSTC sont conformes à la loi — comme il est stipulé à l'alinéa 273.63(2)*a*) de la *Loi sur la défense nationale*; et
- m'assurer que les activités du CSTC menées sous le régime d'une autorisation ministérielle sont dûment autorisées — comme l'établit le paragraphe 273.65(8) de la *Loi sur la défense nationale*.

Les résultats

Chaque année je présente un énoncé de mes constatations concernant la légalité des activités du Centre. Globalement, je suis en mesure d'affirmer que les activités examinées cette année étaient conformes à la loi. Je n'ai formulé aucune recommandation pour cette année. Toutefois, j'ai fait nombre de suggestions visant à améliorer certaines politiques et pratiques et je m'emploierai à en faire le suivi.

À certains égards, l'année a été décevante en raison de retards qui nous ont empêchés de procéder à certains examens. Le Centre n'a pas fourni le même niveau d'appui à mon Bureau pour ces examens, ce qui a entraîné des retards excessifs. Il s'est engagé à corriger la situation. Les directives ministérielles imposent d'ailleurs au chef du Centre l'obligation d'appuyer les examens du commissaire.

conforme à la loi et la mesure dans laquelle il prend les moyens de protéger la vie privée des Canadiens.

Le modèle logique de l'**annexe E** présente un organigramme de notre programme d'examen (p. 50).

Les examens horizontaux portent sur les processus communs à l'ensemble des méthodes de collecte de renseignements électromagnétiques étrangers du CSTC ou des activités de protection des technologies de l'information menées en vertu d'une autorisation ministérielle. Par exemple, les processus en vertu desquels le Centre :

- identifie et choisit des entités d'intérêt pour le renseignement étranger et dirige ses activités vers elles;
- utilise, partage, présente dans des rapports, conserve ou détruit les renseignements interceptés; et
- prend des mesures pour protéger les communications privées interceptées fortuitement ainsi que l'information concernant l'identité de Canadiens.

Recommandations

Depuis 1997, mes prédécesseurs et moi-même avons présenté au ministre de la Défense nationale 68 rapports d'examen classifiés. Au total, ces rapports renfermaient 133 recommandations. Le Centre a souscrit à 93 p.100 (124 sur 133) de ces recommandations et il a pris ou prend actuellement des mesures pour y donner suite. En raison notamment des recommandations, le Centre a suspendu certaines activités pour réexaminer la façon dont elles sont conduites et restructurer les processus et les pratiques qui les sous-tendent. Au cours de l'année écoulée, le Centre a terminé le travail donnant suite à une recommandation antérieure et je fais le suivi de 15 recommandations que le Centre s'emploie à mettre en œuvre. J'attends la réponse du ministre à une recommandation liée à la protection de la vie privée que j'ai formulée en 2010-2011.

On trouvera sur le site web du Bureau la liste des 68 rapports d'examen classifiés présentés au ministre de la Défense nationale (www.ocsec-bccst.gc.ca).

Exigences ministérielles : Je m'attends à ce que le Centre mène ses activités en accord avec les instructions ministérielles, c'est-à-dire conformément à toutes les exigences ou limites précisées dans une autorisation ou une directive ministérielle.

Politiques et procédures : Je m'attends à ce que le Centre dispose de politiques et de procédures pertinentes pour orienter ses activités et donner des consignes suffisantes sur les obligations en vertu de la loi et les exigences ministérielles, notamment en matière de protection de la vie privée des Canadiens. Je m'attends à ce que les employés soient au courant des politiques et procédures et qu'ils s'y conforment. Je m'attends aussi à ce que le Centre utilise des mécanismes de contrôle de gestion efficaces pour assurer le maintien de l'intégrité de ses opérations et de leur conformité à la loi. Le Centre doit être en mesure de rendre compte des décisions prises et de justifier toute information liée à la conformité et à la protection de la vie privée des Canadiens.

Mes rapports d'examen décrivent les activités et les pratiques du Centre et font état des constatations auxquelles j'en arrive eu égard à ces critères. Ces rapports peuvent également indiquer la nature et l'importance des dérogations observées par rapport à ces critères. Dans certains cas, je formule des recommandations à l'intention du ministre qui visent à corriger les écarts entre les activités du Centre et les attentes suscitées par les critères d'examen. Je surveille la façon dont le Centre donne suite aux recommandations et répond aux constatations négatives. J'examine aussi toute question identifiée dans un rapport antérieur comme nécessitant un suivi.

Le processus d'examen est cumulatif. Depuis sa création en 1996, le Bureau a développé une expertise particulière en rapport avec le mandat et les activités uniques du CSTC. À chaque examen, le Bureau enrichit sa connaissance des activités du Centre et perfectionne en conséquence sa propre méthodologie. L'un des changements mis en œuvre ces dernières années concerne l'introduction des examens horizontaux — à savoir l'examen des processus en vertu desquels le Centre choisit ses cibles de renseignement étranger et utilise, partage, présente dans des rapports, conserve ou détruit les renseignements interceptés qui sont communs à chacune des activités ou catégories d'activités. Cette approche a permis d'effectuer des examens en plus grande profondeur. Mon Bureau passe en revue chacun de ces processus communs pour déterminer si le Centre se

Le risque est évalué compte tenu de divers facteurs, entre autres :

- les contrôles exercés par le CSTC sur l'activité pour assurer la conformité aux obligations légales, aux exigences ministérielles et aux politiques du Centre;
- la question de savoir si l'activité peut impliquer des communications privées ou de l'information concernant des Canadiens;
- la nouveauté de l'activité, si elle a subi d'importants changements ou le temps écoulé depuis la dernière fois où elle a fait l'objet d'un examen en profondeur;
- la survenance d'importants changements touchant les autorisations ou les technologies se rapportant à l'activité;
- le suivi des constatations ou des conclusions que les commissaires ont pu formuler; et
- les enjeux soulevés dans le domaine public.

Méthode et critères d'examen

Lorsqu'il procède à un examen, mon Bureau passe en revue les dossiers sur papier et électroniques du Centre, ses politiques et ses procédures, et les avis juridiques reçus du ministère de la Justice. Mon équipe requiert la tenue de séances d'information et de démonstrations portant sur des activités particulières, s'entretient avec des gestionnaires et des employés du Centre et observe directement les opérateurs et les analystes pour vérifier la façon dont ils effectuent leur travail. Mon équipe est en mesure, en la comparant au contenu des systèmes et des bases de données, de vérifier l'exactitude de l'information recueillie. Le travail des vérificateurs internes et des évaluateurs du Centre peut également étayer les examens.

Chaque examen comporte une évaluation des activités du Centre selon une série de critères standard, décrits ci-après, relatifs aux obligations légales, aux exigences ministérielles et aux politiques et procédures du Centre. Chaque examen peut comporter des critères supplémentaires selon les besoins.

> **Obligations en vertu de la loi** : Je m'attends à ce que le Centre mène ses activités en conformité avec la *Loi sur la défense nationale*, la *Loi sur la protection des renseignements personnels,* le *Code criminel,* la *Charte canadienne des droits et libertés,* et toute autre législation pertinente, et en conformité avec les avis du ministère de la Justice.

LE BUREAU DU COMMISSAIRE ET LE PROCESSUS D'EXAMEN

Je suis épaulé dans mon travail par un effectif de huit personnes, auquel s'ajoutent plusieurs experts-conseils, recrutés sur une base contractuelle en fonction des besoins. En 2011-2012, les dépenses du Bureau se sont élevées à 1 942 429 $, ce qui s'inscrit dans les limites du budget alloué par le Parlement. Des travaux d'agrandissement des locaux que j'occupe sont en cours et je disposerai d'une plus grande superficie qui me permettra de recruter des employés supplémentaires.

L'**annexe D** présente l'état des dépenses du Bureau du commissaire du Centre de la sécurité des télécommunications pour 2011-2012 (p. 49).

Objectif de l'examen

L'objectif de l'examen est de me permettre de fournir au ministre de la Défense nationale et, en fait, à tous les Canadiens, l'assurance que le Centre se conforme à la loi et protège la vie privée des Canadiens. Si je découvrais un cas où le Centre pourrait à mon avis ne pas s'être conformé à la loi, je serais tenu d'en informer le ministre de la Défense nationale et le procureur général du Canada.

Sélection des activités visées par l'examen

À l'appui de mes examens, j'adopte une approche de prévention axée sur le risque. Je dispose d'un plan de travail triennal qui est mis à jour deux fois par an et je m'appuie sur de nombreuses sources pour l'élaborer. Mes employés et moi participons régulièrement à des séances d'information que le Centre organise et qui portent sur de nouvelles activités ainsi que sur des changements touchant les activités en cours. Je passe également en revue le rapport annuel que le chef du Centre remet au ministre de la Défense nationale et dans lequel il fait état des priorités et des initiatives du Centre ainsi que des questions juridiques, stratégiques et de gestion qui sont significatives. J'ai ensuite recours à une série de critères qui m'aident à choisir et à hiérarchiser les activités du Centre en fonction des domaines où le risque de non-conformité à la loi est le plus élevé, notamment au chapitre du respect de la vie privée des Canadiens.

Information sur l'identité de Canadiens

Les rapports du Centre peuvent renfermer de l'information permettant d'identifier un Canadien si cette information est jugée essentielle à la compréhension des rapports. Toutefois, l'identité même de ce Canadien doit être supprimée et remplacée par une mention générale du type « un Canadien » ou « une personne morale canadienne ». Lorsqu'il reçoit une demande subséquente de divulgation de précisions sur l'information supprimée, le Centre doit vérifier que le ministère ou organisme gouvernemental dont elle émane dispose à la fois de l'autorisation et d'une justification opérationnelle pour obtenir ce genre de renseignements. Ce n'est qu'une fois satisfait que le Centre fournit l'information. Annuellement, je choisis et j'examine un échantillon de ces divulgations pour vérifier que le Centre se conforme à la loi et met en pratique des mesures de protection de la vie privée des Canadiens.

Collaboration internationale

Le Centre et ses partenaires étrangers les plus proches — National Security Agency des États-Unis, Government Communications Headquarters du Royaume-Uni, Defence Signals Directorate de l'Australie et Government Communications Security Bureau de la Nouvelle-Zélande — respectent les lois des uns et des autres en s'engageant à ne pas cibler les communications des citoyens de ces autres pays. Il est interdit au Centre de demander à un partenaire étranger d'entreprendre des activités que le Centre lui-même n'est pas autorisé à mener. Dans le cadre de mes examens, j'examine comment le Centre coopère avec ses alliés pour m'assurer qu'il le fait en conformité à la loi.

Formation au Centre

Grâce au programme de formation du Centre, le personnel est sensibilisé aux exigences et aux politiques relatives à la légalité et à la protection de la vie privée des Canadiens. Tout nouvel employé du Centre assiste à un cours d'apprentissage de base, qui l'informe notamment des obligations qui lui incombent en matière de protection de la vie privée. Par ailleurs, les employés du Centre qui sont chargés de certaines opérations sont tenus de participer à des séances d'information sur les exigences de la loi avant de commencer leur travail et au moins une fois par année par la suite. Au cours de mes examens, je vérifie si cette formation est efficace en interrogeant les employés du Centre sur leur compréhension de leurs obligations. L'**annexe C** renferme le libellé des articles pertinents de la *Loi sur la défense nationale* se rapportant au rôle et au mandat du Centre (p. 47).

Les rapports du chef à cet égard constituent un des mécanismes me permettant de me tenir au fait des activités du Centre. Ils m'aident également à élaborer le plan de travail de mes examens.

Une directive ministérielle en particulier, la Directive de juin 2001 sur la vie privée des Canadiens, renforce les obligations stipulées dans la *Loi sur la défense nationale* et les autorisations ministérielles. Elle exige que le Centre adopte des mesures pour minimiser l'interception fortuite de communications privées. Elle énonce que le Centre peut conserver l'information sur des Canadiens et faire rapport sur cette information, pourvu que des critères spécifiques et des mesures appropriées soient en place pour le traitement, la conservation et la destruction de cette information. Le traitement de cette information doit être conforme à la *Charte canadienne des droits et libertés* et à la *Loi sur la protection des renseignements personnels*. D'autres directives ministérielles fournissent une orientation sur des activités particulières du Centre.

La politique opérationnelle du Centre, intitulée *Protéger la vie privée des Canadiens et assurer la conformité à la loi et mener ses activités en accord avec les exigences ministérielles*, s'applique à quiconque mène des activités sous l'autorité du Centre, y compris ses employés et le personnel militaire. Elle énonce les mesures détaillées à prendre pour assurer la conformité à la loi et pour protéger la vie privée des Canadiens dans l'utilisation et la conservation des renseignements interceptés. Nombre d'autres politiques et procédures renferment des exigences détaillées et fournissent des directives sur des activités particulières du Centre et sur les mesures propres à protéger la vie privée. J'examine les activités du Centre pour m'assurer qu'elles soient conformes aux directives ministérielles ainsi qu'aux politiques et procédures du Centre.

Information sur les Canadiens : Tout renseignement personnel (au sens de la *Loi sur la protection des renseignements personnels*) à propos d'un Canadien, y compris une personne morale canadienne.

- s'il s'agit de renseignements étrangers au sens de la *Loi sur la défense nationale* et s'ils sont en conformité avec les priorités du gouvernement du Canada en matière de renseignements;
- s'ils sont essentiels pour protéger la vie ou la sécurité de personnes, quelle qu'en soit la nationalité;
- s'ils renferment de l'information sur des activités criminelles graves se rapportant à la sécurité du Canada; ou
- s'ils sont essentiels pour identifier, isoler ou prévenir des activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada.

Lorsqu'une autorisation ministérielle arrive à terme, le chef du Centre doit faire rapport au ministre de la Défense nationale relativement aux communications privées qui ont été interceptées de façon fortuite pendant que l'autorisation était en cours. Ce rapport doit préciser le nombre de communications privées qui ont été utilisées ou conservées sur la base, comme l'exige la loi, qu'elles étaient essentielles pour les affaires internationales, la défense ou la sécurité, ou encore qu'elles permettaient d'identifier, isoler ou prévenir des activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada. Ce rapport doit également faire état du nombre et de la valeur de tous les rapports sur les renseignements étrangers produits à partir des renseignements tirés des communications privées.

J'examine les rapports que le chef présente au ministre, je jauge le nombre de communications privées interceptées fortuitement et je vérifie la façon dont le Centre a traité et utilisé ces communications. Je suis en mesure d'examiner toutes et chacune des communications privées que le Centre utilise et conserve.

Directives et politiques

Le Ministre peut, par écrit, donner au chef des directives portant sur son mandat et sur les activités du Centre. La directive ministérielle de juin 2001 sur le cadre de responsabilisation du Centre de la sécurité des télécommunications établit le régime de reddition des comptes du Centre, lequel comprend l'obligation de rendre compte annuellement au ministre de la Défense nationale des priorités et initiatives du Centre, de même que des problèmes importants d'ordre juridique, stratégique et de gestion.

d'autorisation susmentionnées sont remplies. Je fais rapport de mon examen au ministre de la Défense nationale.

Partie *c*) du mandat du Centre

Pour que le Centre puisse aider les organismes fédéraux chargés de l'application de la loi et de la sécurité à exercer leurs activités, la *Loi sur la défense nationale* exige que ces organismes montrent d'abord qu'ils sont dûment habilités par la loi — en vertu, par exemple, d'une autorisation ou d'un mandat — pour mener les activités en question. Le CSTC est alors assujetti aux mêmes lois et restrictions que celles régissant les organismes qu'il aide plutôt qu'aux trois limites stipulées dans la *Loi sur la défense nationale* et susmentionnées. Il est important de rappeler que les activités menées par le Centre en vertu de la partie *c*) de son mandat ne sont pas soumises à l'exigence d'une autorisation ministérielle.

EXIGENCES MINISTÉRIELLES ET POLITIQUES DU CENTRE VISANT LA PROTECTION DE LA VIE PRIVÉE DES CANADIENS

Outre les limites définies dans la *Loi sur la défense nationale,* les activités de collecte de renseignements électromagnétiques étrangers et de sécurité des technologies de l'information du Centre sont visées par différentes mesures prescrites par le ministre ou définies par le Centre lui-même qui sont destinées à protéger la vie privée des Canadiens lors de l'utilisation et la conservation des renseignements interceptés.

Les secteurs de programme relatifs aux renseignements électromagnétiques étrangers et à la sécurité des technologies de l'information du Centre disposent de sections spécialisées chargées quotidiennement de la conformité et de la surveillance. Ces deux sections constituent des volets importants des mécanismes de contrôle de gestion et de responsabilisation du CSTC et je me penche sur l'efficacité de ces mécanismes au cours de mes examens.

Traitement des communications privées interceptées

Le Centre doit utiliser les moyens dont il dispose pour réduire, dans la mesure du possible, l'interception fortuite de communications privées de Canadiens. Mais lorsqu'il y a telle interception, le Centre doit détruire ces communications, sauf dans les cas suivants :

Conditions applicables à l'autorisation ministérielle

Pour émettre une autorisation ministérielle visant la collecte de renseignements électromagnétiques étrangers, le ministre doit être convaincu que :

- l'interception visera des entités étrangères situées à l'extérieur du Canada;
- les renseignements ne peuvent raisonnablement être obtenus d'une autre manière;
- la valeur des renseignements étrangers que l'on espère obtenir justifie l'interception envisagée; et
- il existe des mesures satisfaisantes pour protéger la vie privée des Canadiens et pour faire en sorte que les communications privées ne soient utilisées ou conservées que si elles sont essentielles pour les affaires internationales, la défense ou la sécurité.

Pour émettre une autorisation ministérielle dans le but de protéger les systèmes ou les réseaux informatiques du gouvernement du Canada, le ministre doit être convaincu que :

- l'interception est nécessaire;
- les renseignements ne peuvent raisonnablement être obtenus d'une autre manière;
- le consentement des personnes dont les communications peuvent être interceptées ne peut raisonnablement être obtenu;
- des mesures satisfaisantes sont en place pour faire en sorte que seuls les renseignements qui sont essentiels pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada seront utilisés ou conservés; et
- des mesures satisfaisantes sont en place pour protéger la vie privée des Canadiens en ce qui concerne l'utilisation et la conservation de ces renseignements.

Chaque année, j'examine toutes les autorisations ministérielles du Centre — dont la période de validité ne peut dépasser une année — pour m'assurer que les activités sont autorisées et que les conditions

Communication privée : « Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine » (article 183 du *Code criminel*).

Autorisations ministérielles

Lorsque le Centre mène ses activités pour acquérir des renseignements électromagnétiques étrangers, il ne peut pas savoir à l'avance avec qui l'entité étrangère ciblée à l'extérieur du Canada peut communiquer. De même, lorsque le Centre mène des activités pour aider à protéger les systèmes informatiques du gouvernement du Canada, il ne peut pas savoir à l'avance qui peut communiquer avec ce système informatique ou par son intermédiaire. Compte tenu de la complexité et de l'interconnectivité de l'infrastructure d'information mondiale, il est inévitable qu'il intercepte un certain nombre de communications privées. C'est pourquoi le Centre a besoin d'une autorisation ministérielle pour mener ces activités — afin de ne pas tomber sous le coup du *Code criminel* au cas où il intercepterait de manière fortuite une communication entrant au Canada ou en sortant, là où une personne s'attendait à parler en privé. Les autorisations ministérielles accordées au Centre se rapportent à une « activité » ou à une « catégorie d'activités » précisées dans les autorisations, c'est-à-dire qu'elles visent expressément une méthode d'acquisition de renseignements électroniques étrangers ou de protection des systèmes informatiques (le comment). Les autorisations ne se rapportent pas à une personne ou à un sujet en particulier (le qui ou le quoi).

Autorisation ministérielle : autorisation écrite du ministre de la Défense nationale accordée au CSTC de façon à ce qu'il ne contrevienne pas au *Code criminel* si — au cours de sa collecte de renseignements électromagnétiques étrangers ou de ses activités reliées à la sécurité des technologies de l'information — il intercepte de manière fortuite une communication privée. Une autorisation peut être en vigueur pour un an au maximum. En 2011-2012, six autorisations de collecte de renseignements électromagnétiques étrangers et deux autorisations relatives à la sécurité des technologies de l'information étaient en vigueur.

LIMITES IMPOSÉES AU CENTRE PAR LA LOI

Parties *a*) et *b*) du mandat du Centre

Les activités du Centre liées à la collecte de renseignements électromagnétiques étrangers et à la protection des renseignements électroniques et des infrastructures d'information importantes pour le gouvernement du Canada sont assujetties à trois limites imposées par la loi visant à protéger la vie privée des Canadiens :

1. Le Centre se voit interdire de viser des Canadiens où qu'ils se trouvent dans le monde, ou toute personne au Canada, quelle que soit sa nationalité;

2. En menant ces activités, il arrive que le Centre intercepte de manière fortuite une communication destinée au Canada ou en provenance du Canada, dans des circonstances telles que son auteur était raisonnablement en droit de s'attendre à ce qu'elle ne soit pas interceptée, ce qui en fait une communication privée au sens du *Code criminel*. En pareil cas, le Centre *peut* utiliser ou conserver la communication privée obtenue de cette manière, mais *uniquement* si elle est essentielle pour les affaires internationales, la défense ou la sécurité, ou pour identifier, isoler ou prévenir des activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement fédéral; et

3. Pour encadrer de manière formelle l'interception fortuite de communications privées au cours de ces activités, la *Loi sur la défense nationale* exige l'autorisation expresse du ministre de la Défense nationale. Le processus est connu sous le nom d'autorisation ministérielle. Le ministre peut autoriser les activités une fois qu'il est convaincu que certaines conditions définies par la loi sont satisfaites, notamment qu'il a obtenu des garanties sur la façon dont ces interceptions fortuites de communications privées seront traitées, le cas échéant.

L'**annexe A** renferme le libellé des articles pertinents de la *Loi sur la défense nationale* et de la *Loi sur la protection de l'information* se rapportant à mon rôle et à mon mandat en tant que commissaire du Centre (p. 41) et l'**annexe B** présente l'historique du Bureau du commissaire du Centre de la sécurité des télécommunications (p. 45).

MANDAT DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS CANADA

Lorsque la *Loi antiterroriste* est entrée en vigueur le 24 décembre 2001, elle a ajouté la partie V.1 à la *Loi sur la défense nationale* et établi le mandat à trois volets du Centre :

> La partie *a*) autorise le Centre à acquérir et à utiliser les renseignements électromagnétiques étrangers en conformité avec les priorités du gouvernement du Canada en matière de renseignement;
>
> La partie *b*) autorise le Centre à aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada; et
>
> La partie *c*) autorise le Centre à fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, notamment pour qu'ils obtiennent et comprennent les communications recueillies en vertu de leurs autorités respectives.

Protection des Canadiens

Le Centre se voit interdire, dans le cadre de ses activités de collecte de renseignements électromagnétiques étrangers ou de sécurité des technologies de l'information, de cibler des Canadiens — où qu'ils se trouvent dans le monde — ou toute personne au Canada.

Informer le ministre

En vertu de mon mandat :

- je fais état des résultats de mes examens dans des rapports classifiés adressés au ministre de la Défense nationale, lequel est responsable du Centre devant le Parlement; et
- je suis tenu de présenter chaque année un rapport non classifié sur mes activités au ministre de la Défense nationale, lequel doit ensuite le déposer au Parlement. Il s'agit ici du 16e rapport annuel.

Mes examens visent essentiellement à vérifier si le Centre se conforme aux exigences que lui imposent la loi, le ministre et ses propres politiques. Si je suis tenu avant tout de faire état des incidents de non-conformité du Centre, une des obligations de mon mandat consiste également à informer le Centre de toute activité qui, à mon avis, pourrait présenter un risque de non-conformité, notamment l'interception illégale d'une communication privée ou toute autre atteinte à la vie privée d'un Canadien. Si je ne suis pas convaincu que le Centre prend en compte comme il se doit mes préoccupations, j'ai le pouvoir et l'obligation d'en faire rapport au ministre de la Défense nationale. Plusieurs de mes rapports incluent des recommandations axées sur la prévention, car mon but est de renforcer les pratiques du Centre qui favorisent la conformité et intègrent des mesures propres à protéger la vie privée des Canadiens. J'estime qu'il est en définitive plus utile de prévenir les activités illégales que de les détecter après coup.

Indépendance

Bien que je présente mes rapports au ministre responsable du Centre, le Bureau du commissaire est indépendant et distinct du ministère de la Défense nationale. Mon mandat d'examen est renforcé par les pouvoirs dont je suis investi en vertu de la *Loi sur les enquêtes.* Ces pouvoirs me garantissent l'accès à toute information et aux employés du Centre et incluent le pouvoir d'assigner à comparaître. L'indépendance de mon mandat est par ailleurs attestée par le mode de financement du Bureau — qui est un organisme autonome bénéficiant de son propre crédit parlementaire plutôt que d'un financement par l'intermédiaire du ministère de la Défense nationale.

Examen des activités du CSTC

L'objet de mon mandat d'examen consiste :

- à m'assurer que les activités que mène le Centre en vertu d'autorisations ministérielles sont bien celles autorisées par le ministre de la Défense nationale;
- à m'assurer que le CSTC se conforme à la loi et, si je pense qu'il pourrait ne pas s'y conformer, en faire rapport au ministre de la Défense nationale et au procureur général du Canada;
- à m'assurer que, dans ses activités de collecte de renseignements électromagnétiques étrangers et à l'appui de la sécurité des technologies de l'information, le CSTC ne cible pas des Canadiens; et
- à m'assurer que le CSTC, dans toutes les activités qu'il entreprend, met en place et applique efficacement des mesures suffisantes de protection de la vie privée des Canadiens.

Conduite d'enquêtes

En vertu de mon mandat, je suis tenu d'entreprendre toute enquête jugée nécessaire par suite d'une plainte formulée par écrit — par exemple pour déterminer si le Centre a mené ou mène une activité non conforme à la loi ou s'il ne prend pas suffisamment de mesures pour protéger la vie privée des Canadiens.

Sur réception d'une plainte écrite, j'évalue si elle pourrait être fondée et si elle relève de mon mandat. Si je détermine qu'une plainte est fondée et relève de mon mandat, j'ai tous les pouvoirs d'un commissaire, en vertu de la partie II de la *Loi sur les enquêtes*, pour obtenir et examiner tous les renseignements détenus par le CSTC. Je peux également interroger — sous serment au besoin – tout employé du CSTC pour établir les faits concernant la plainte. Je préviens le plaignant, le ministre de la Défense nationale et le chef du Centre du résultat d'une enquête officielle sur une plainte. Si j'estime que le Centre pourrait ne pas avoir respecté la loi, j'en ferais rapport au ministre ainsi qu'au procureur général du Canada.

MANDAT DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

Aperçu

- Le mandat dont j'ai été investi (de même que celui du CSTC) est défini à la partie V.1 de la *Loi sur la défense nationale*.
- J'exerce mes activités de façon indépendante du gouvernement.
- Je présente des rapports classifiés détaillés de mes examens du CSTC au ministre de la Défense nationale.
- Je formule des recommandations visant à réduire le risque de non-conformité à la loi du CSTC et à renforcer ses pratiques à l'appui de la protection de la vie privée des Canadiens.

Le mandat dont j'ai été investi en vertu de la *Loi sur la défense nationale* comprend trois fonctions principales :

1. **Procéder à des examens concernant les activités du CSTC** pour en contrôler la légalité;

2. **Faire les enquêtes** que j'estime nécessaires à la suite de plaintes concernant le CSTC; et

3. **Informer le ministre** de la Défense nationale et le procureur général du Canada de toute activité du CSTC qui, à mon avis, pourrait ne pas être conforme à la loi.

J'ai en outre pour mandat, en vertu de la *Loi sur la protection de l'information,* de recevoir de l'information émanant de personnes astreintes au secret à perpétuité qui souhaitent communiquer des renseignements opérationnels spéciaux du CSTC en faisant valoir la primauté de l'intérêt public. À ce jour, aucune affaire de ce genre n'a jamais été signalée à un commissaire.

John Forster, un haut fonctionnaire d'expérience, assume la direction du Centre depuis le 30 janvier 2012. Je l'ai rencontré à quelques reprises et je décèle déjà chez lui les attributs de son prédécesseur. Je suis confiant que nos relations seront empreintes de courtoisie et de respect. Mon équipe et moi avons organisé pour le nouveau chef une séance intensive d'information, dans le but de rendre le plus concret possible à ses yeux le rôle de surveillance qui nous est dévolu par la loi.

Par ailleurs, jusqu'au 16 novembre 2011, le Centre était en quelque sorte une institution sous tutelle relevant à la fois du sous-ministre de la Défense nationale, pour son administration et ses finances, et du conseiller en matière de sécurité nationale auprès du Premier ministre, pour ses opérations et ses politiques. Ce jour-là, le Centre est devenu une entité autonome s'inscrivant dans le portefeuille du ministre de la Défense nationale et ayant statut de ministère. Son chef a pris rang d'administrateur général et relève directement du ministre.

Je ne m'attends pas à ce que ce changement de statut ait un impact sur mes relations avec le Centre. Cependant, j'étais d'avis que l'obligation de faire rapport au conseiller du Premier ministre permettait d'apporter aux opérations et aux politiques du Centre une perspective gouvernementale plus globale en matière de sécurité nationale, et je m'assurerai que l'autonomie nouvelle du Centre ne soit pas cause de relâchement dans l'application de ses mécanismes de contrôle en matière de reddition de compte et de conformité.

Cette collaboration accrue entre le Centre et le SCRS exige à son tour une collaboration accrue entre les organismes qui les surveillent. Or, ce n'est pas là une tâche facile car les lois qui régissent les organismes de surveillance établissent des compétences particulièrement étanches qui n'incitent pas à la mise en commun d'énergies et de ressources. Je me suis employé ces derniers temps à trouver des façons inédites de rendre davantage complémentaires les examens qu'entreprennent chacun de leur côté mon Bureau et le Comité de surveillance des activités de renseignement de sécurité (Comité de surveillance), pour m'assurer qu'aucune activité n'échappe à la surveillance. Le paragraphe 273.63(6) de la *Loi sur la défense nationale* permet au gouverneur en conseil de m'autoriser à me « livrer à toute activité connexe ». L'article 54 de la *Loi sur le Service canadien du renseignement de sécurité* permet au ministre de la Sécurité publique et de la Protection civile de demander au Comité de surveillance « un rapport spécial sur toute question qui relève de sa compétence ». Je suis d'avis que mon Bureau et le Comité de surveillance pourraient, en vertu de ces dispositions, être invités à mener de manière conjointe ou complémentaire une enquête sur certaines activités qui concernent à la fois le Centre et le SCRS. Il s'agirait là d'une démarche qui se situerait dans l'esprit des recommandations formulées par le juge Dennis O'Connor dans son deuxième rapport de la *Commission d'enquête sur les actions des responsables Canadiens relativement à Maher Arar*, qui traite du système de surveillance des organismes de sécurité et de renseignement au Canada.

Ce rapport annuel ne serait pas complet si je n'y soulignais pas certains changements majeurs qui sont survenus dans la haute direction du Centre et dans le statut de ce dernier.

En janvier dernier, John Adams, qui exerçait la fonction de chef du Centre depuis six ans, a été nommé conseiller supérieur auprès du Bureau du Conseil privé et est devenu titulaire du « Skelton-Clark Fellow to the Queen's University of Policy Studies ». Je suis en mesure de témoigner jusqu'à quel point il a su développer au sein du Centre une culture de respect de la vie privée qui facilite grandement mon travail. Il y aura toujours, bien sûr, entre un organisme de surveillance et l'organisme sous surveillance, un climat inévitable et nécessaire de tension. Le défi que doivent alors relever les chefs des deux organismes est de faire en sorte que cette tension soit saine et productive. Tel m'apparaît avoir été le cas en l'espèce.

rôles respectifs du Centre et du SCRS. Je constate en effet qu'il y a souvent méprise quant à ces rôles.

Le Centre, lorsqu'il agit de sa propre initiative, n'a pas le droit, de par sa loi constituante, de viser qui que ce soit au Canada non plus qu'aucun Canadien hors Canada. Cependant, le Centre a aussi le mandat d'apporter son aide à des organismes tels le SCRS, ce qui peut l'amener à s'intéresser, sur demande, à un Canadien ou à une personne se trouvant au Canada. Lorsque le Centre fournit une telle assistance, il est assujetti aux lois qui régissent l'organisme qui a fait la demande.

Puisque le SCRS, de par sa loi habilitante, s'intéresse à des menaces envers la sécurité du Canada et mène ses enquêtes en utilisant des méthodes qui conduisent à l'interception de communications privées, le risque d'atteinte à la vie privée des Canadiens est inhérent à ses activités et le Parlement a voulu que ces activités ne puissent avoir lieu sans l'obtention préalable d'un mandat judiciaire. En conséquence, lorsque le SCRS, dans l'exécution de ce mandat judiciaire, demande l'aide du Centre, le Centre ne fait en réalité que participer à une activité déjà autorisée par mandat judiciaire. Il serait superflu d'exiger à ce moment l'obtention d'un autre mandat. Mes prédécesseurs ont examiné l'assistance portée au SCRS par le Centre. J'ai entrepris cette année un examen en profondeur, que je compléterai au cours des prochains mois, de certaines activités que mène le Centre lorsqu'il agit à la demande du SCRS.

Par ailleurs, puisque le Centre ne cible que des non-Canadiens hors Canada, les interceptions de communications privées qui impliqueraient des Canadiens sont tout aussi fortuites qu'imprévisibles. Le risque d'atteinte à la vie privée de Canadiens, au moment de l'interception, n'est dès lors qu'aléatoire et le Parlement s'est contenté d'exiger que ces activités du Centre qui peuvent fortuitement mener à une atteinte à la vie privée de Canadiens fassent l'objet, non pas d'un mandat judiciaire, mais d'une autorisation dite ministérielle émise par le ministre de la Défense nationale. Cette autorisation ministérielle ne constitue pas pour autant un chèque en blanc : elle est assortie d'exigences importantes que la loi impose et d'autres que le ministre peut prescrire, pour s'assurer que s'il advenait que la vie privée d'un Canadien soit engagée, des mesures soient en place pour la protéger.

MESSAGE DU COMMISSAIRE

Le but premier de ce rapport est d'informer le ministre de la Défense nationale des activités auxquelles je me suis adonné au cours de l'exercice qui s'est terminé le 31 mars 2012. Je ferai état aussi bien des résultats des examens que j'ai effectués au cours de l'année relativement aux opérations du Centre de la sécurité des télécommunications Canada (le Centre ou le CSTC), que des projets d'examen qui sont en cours et de ceux que je compte entreprendre dans les prochains mois. Je ferai état également des autres activités que moi-même et mon Bureau avons menées, notamment celles visant à nous tenir au courant des plus récents développements survenus au Canada et ailleurs en matière de surveillance d'organismes de sécurité et de renseignement.

Aux deux tiers de mon mandat triennal, force m'est de constater que le grand public, et parfois même ses membres qui se disent spécialisés, continuent, par ignorance, de se méprendre sur les rôles respectifs des divers organismes canadiens de renseignement et, par voie de conséquence, sur les rôles respectifs des divers organismes de surveillance. Cette ignorance s'explique. Le caractère secret des activités des organismes de renseignement fait en sorte que toute tentative de vulgarisation se heurte à une culture du silence qui veut que l'on taise même ce qui est connu ou ce qui pourrait l'être. Pour paraphraser une expression consacrée, la peur que l'on voie certains arbres est telle qu'il n'est pas permis de décrire la forêt. À mon avis, il est possible, sans entrer dans des détails qu'il serait inapproprié de divulguer, d'employer un vocabulaire plus simple et plus compréhensible et d'ainsi faire en sorte que les débats publics ne s'engagent pas sur de fausses prémisses.

Dans mon message de l'an dernier, j'ai brièvement décrit les mandats respectifs du Centre et de mon Bureau. Je reviens à la charge, cette année, de manière plus détaillée, dans mon rapport.

La technologie se développe à un rythme époustouflant. L'expertise en technologie des télécommunications du Centre l'amène, dans le cadre de son mandat, à fournir une aide à d'autres membres de la collectivité canadienne de la sécurité et du renseignement, notamment le Service canadien du renseignement de sécurité (SCRS). Je voudrais cette année, dans la poursuite de mes efforts de vulgarisation, apporter des précisions quant aux

BIOGRAPHIE DE L'HONORABLE ROBERT DÉCARY, C.R.

L'honorable Robert Décary, c.r., a été nommé Commissaire du Centre de la sécurité des télécommunications le 18 juin 2010.

Le commissaire Décary est né à Montréal en 1944. Il a fait ses études au Collège Jean-de-Brébeuf (B. A.), à l'Université de Montréal (LL.L.) et à l'Université de Londres (LL.M.). Il est devenu membre du Barreau du Québec en 1967 et a reçu, en 1986, le titre de conseiller de la reine.

Au cours de sa carrière consacrée à la chose publique, au droit et au journalisme, il a notamment été adjoint spécial auprès de l'honorable Mitchell Sharp, alors secrétaire d'État aux Affaires extérieures du Canada (1970-1973), co-directeur de la recherche à la Commission de l'unité canadienne, la Commission Pepin-Robarts (1978-1979), et membre du Comité de rédaction constitutionnelle française du ministère fédéral de la Justice (1985-1990).

Il a pratiqué le droit à Montréal, puis à Gatineau, où il s'est spécialisé, au sein du cabinet Noël, Décary, dans la représentation de nombreux cabinets d'avocats et du procureur général du Québec auprès de la Cour suprême du Canada.

Il a écrit de nombreuses chroniques dans *Le Devoir* et *La Presse* et il a contribué à maintes revues et ouvrages juridiques. Il est l'auteur d'un *Aide-mémoire sur la Cour suprême du Canada* (1988) et de *Chère Élize (ou la grande et la petite histoire du rapatriement)* (1983).

Il a été membre de la Cour d'appel fédérale de 1990 à 2009. En 2009, il était nommé arbitre du Tribunal arbitral du sport (Lausanne) et en 2010, il devenait membre du Centre de règlement des différends sportifs du Canada.

Plaintes concernant les activités du Centre /34

Mandat sous le régime de la *Loi sur la protection de l'information* /35

Activités du Bureau du commissaire /35

Plan de travail — Examens en cours et prévus /38

L'année à venir /38

Annexe A : Extraits de la *Loi sur la défense nationale* et la *Loi sur la protection de l'information* se rapportant au mandat du commissaire du Centre de la sécurité des télécommunications /41

Annexe B : Historique du Bureau du commissaire du Centre de la sécurité des télécommunications /45

Annexe C : Extraits de la *Loi sur la défense nationale* se rapportant au mandat du Centre de la sécurité des télécommunications /47

Annexe D : État des dépenses 2011-2012 /49

Annexe E : Programme d'examen du Bureau du commissaire — Modèle logique /50

TABLE DES MATIÈRES

Biographie de l'honorable Robert Décary, c.r. /2

Message du commissaire /3

Mandat du commissaire du Centre de la sécurité des télécommunications /7

Mandat du Centre de la sécurité des télécommunications Canada /10

Limites imposées par la loi au CSTC /11

Exigences ministérielles et politiques du Centre visant la protection de la vie privée des Canadiens /14

Le Bureau du commissaire et le processus d'examen /18

Aperçu des constatations 2011-2012 /22

Faits saillants des sept rapports présentés au ministre en 2011-2012 /23

1. Conservation et destruction par le CSTC des communications interceptées ou copiées /23

2. Activités du centre des opérations du CSTC et de collecte de renseignements électromagnétiques étrangers particuliers menées en 2010 /25

3. Mise à jour concernant l'examen en cours du partage des renseignements électromagnétiques étrangers du CSTC avec des partenaires étrangers /26

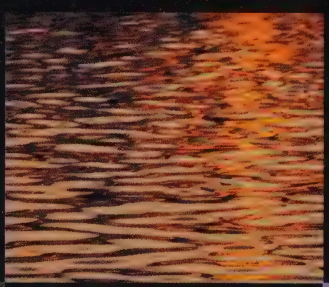
4. Examen combiné annuel des autorisations ministérielles relatives aux renseignements électromagnétiques étrangers du Centre /28

5. Examen annuel d'un échantillon de renseignements concernant l'identité de Canadiens divulgués aux clients du gouvernement du Canada pour l'année 2011 /30

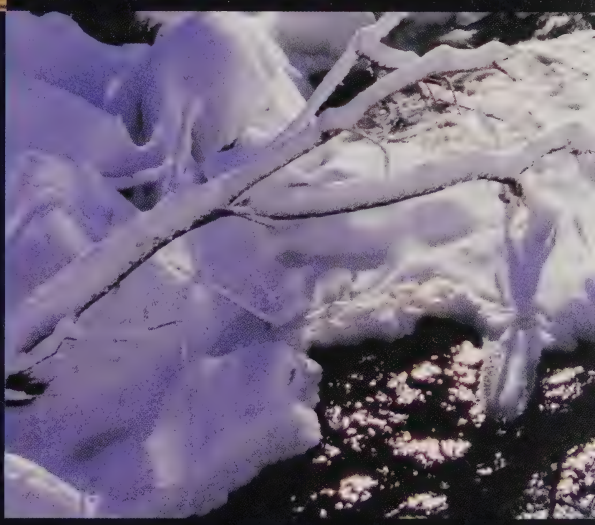
6. et 7. Examen annuel des incidents signalés par le Centre en 2010 et 2011 qui ont touché ou auraient pu toucher la vie privée de Canadiens ainsi que des mesures prises par le Centre pour régler le problème /32

Commissaire
du Centre
de la sécurité
des télécommunications

Rapport annuel







2011-2012

Canada

CA1
ND 800
-S16

Government
Publications



COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

ANNUAL REPORT 2012-2013

Canada

Office of the Communications Security
Establishment Commissioner
P.O. Box 1984, Station "B"
Ottawa, Ontario
K1P 5R5

Tel.: 613-992-3044
Fax: 613-992-4096
Website: www.ocsec-bccst.gc.ca

© Minister of Public Works and
Government Services 2013
Cat. No. D95-2013
ISSN 1206-7490

Cover design: Cameron Fraser



Communications Security
Establishment Commissioner

The Honourable Robert Décary, Q.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Robert Décary, c.r.

June 2013

SEP 10 2013
University of Toronto

Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Minister:

Pursuant to subsection 273.63(3) of the *National Defence Act*, I am pleased to submit to you my annual report on my activities and findings for the period of April 1, 2012, to March 31, 2013, for your submission to Parliament.

Yours sincerely,

Robert Décary

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

TABLE OF CONTENTS

Biography of the Honourable Robert Décary, Q.C. /2

Commissioner's Message: A Summary at the End of My Term /3

Mandate of the Communications Security Establishment Commissioner /9

Commissioner's Office /15

Impact of Commissioners' Recommendations /16

Overview of 2012–2013 Findings and Recommendations /17

Highlights of the Six Reviews Submitted to the Minister in 2012–2013 /20

1. Review of certain foreign signals intelligence activities /20
2. CSEC assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the *CSIS Act* /21
3. Review of CSEC IT security activities not conducted under a ministerial authorization /26
4. Review of CSEC's 2010–2011 and 2011–2012 foreign signals intelligence ministerial authorizations /29
5. Annual review of a sample of disclosures of Canadian identity information to Government of Canada clients /32
6. Annual review of incidents and procedural errors identified by CSEC in 2012 that affected or had the potential to affect the privacy of Canadians and measures taken by CSEC to address them /34

Complaints About CSEC Activities /36

Duty Under the *Security of Information Act* /36

Activities of the Commissioner's Office /36

Work Plan — Reviews Under Way and Planned /38

In Closing /39

Annex A: Commissioner's Office Review Program — Logic Model /41

Annex B: Excerpts from the *National Defence Act* and the *Security of Information Act* Related to the Commissioner's Mandate /43

Annex C: 2012–2013 Statement of Expenditures /47

BIOGRAPHY OF THE HONOURABLE ROBERT DÉCARY, Q.C.

The Honourable Robert Décary, Q.C., was appointed Commissioner of the Communications Security Establishment on June 18, 2010, for a three-year term.

Commissioner Décary was born in Montréal in 1944. He received his education at Collège Jean-de-Brébeuf (BA), at Université de Montréal (LL.L.) and the University of London (LL.M.). He was called to the Barreau du Québec in 1967 and named Queen's Counsel in 1986.

In the course of a career dedicated to public office, the law and journalism, he was Special Assistant to the Honourable Mitchell Sharp (then Canada's Secretary of State for External Affairs) (1970–1973), Co-Director for Research on the Task Force on Canadian Unity, the Pepin-Robarts Commission (1978–1979) and member of the French Constitutional Drafting Committee of the federal Department of Justice (1985–1990).

He practised law in Montréal, then in Gatineau, where, in the firm Noël, Décary, he specialized in representing many law offices and the Attorney General of Québec before the Supreme Court of Canada.

He has written a number of feature articles for *Le Devoir* and *La Presse*, and has contributed to many legal journals and textbooks. He is the author of *Aide-mémoire sur la Cour suprême du Canada* (1988) and of *Chère Élize* (or *The Long and the Short History of the Repatriation*) (1983).

He was a member of the Federal Court of Appeal from 1990 to 2009. In 2009, he was appointed arbitrator of the Court of Arbitration for Sport in Lausanne, Switzerland, and in 2010 he became a member of the Sport Dispute Resolution Centre of Canada.

COMMISSIONER'S MESSAGE: A SUMMARY AT THE END OF MY TERM

When the Minister of National Defence tables this annual report before Parliament, I will have completed my three-year term as Communications Security Establishment (CSE) Commissioner. For personal reasons I declined an offer to renew my mandate. This message affords me an opportunity to reflect on my time as the head of the Office of the CSE Commissioner.

Reports and recommendations

During my tenure as Commissioner I submitted to the Minister of National Defence 19 review reports, covering almost every aspect of the activities of Communications Security Establishment Canada (CSEC), including those carried out under ministerial authorizations or at the request of law enforcement and security agencies. Among the activities reviewed were those relating to the collection of foreign signals intelligence, the protection of electronic information and information infrastructures considered important by the Government of Canada, and technical and operational assistance provided by CSEC, notably to the Canadian Security Intelligence Service (CSIS). My reports contained 12 recommendations.

The integrity of the review process and the credibility of the Commissioner's office depend in large part on the follow-up by the office of CSEC's implementation of Commissioners' recommendations. I am pleased to note that since 1997, fully 92 percent (127 of 138) of Commissioners' recommendations in 74 classified reports submitted to the Minister have been accepted and implemented, or are being addressed. This means, *inter alia* that measures to protect the privacy of Canadians are continually being adapted and refined to reflect the ever-changing technological and operational environment in which CSEC must work. Indeed, some Commissioners' recommendations have resulted in CSEC suspending certain activities to re-examine how the activities are conducted and, in other instances, have led to important improvements to CSEC policies and practices.

Maintaining healthy relations with CSEC

It strikes me as vital that an organization under independent review and the review body itself cultivate a relationship built on respect and good faith. By law, CSEC must take measures to protect the privacy of persons in Canada and Canadians, wherever in the world they may be. By law, the Commissioner must ensure that CSEC meets this obligation. The protection of privacy is therefore a shared objective of our two organizations. I also consider it essential that our relationship be one of complementarity rather than superiority. With my years of experience, I see the office more as CSEC's conscience than as a sword of Damocles, and I believe that CSEC increasingly sees it this way as well.

I can say with confidence that CSEC's Chiefs during my time as Commissioner, John Adams initially and then John Forster, have spared no effort to instill within CSEC a culture of respect for the law and for the privacy of Canadians. Both men have been honest in their dealings with me, sometimes tough, but always acting in good faith.

Transparency

From the start of my time as Commissioner, I have sought to demystify, within the unavoidable constraints of national security and public safety, the culture of secrecy pervading the activities of security and intelligence agencies. I believe I have succeeded to some degree, based on the feedback that my annual reports have been more informative, more understandable, and have brought clarity to many of the activities of my office and of CSEC. Much remains to be done, but I believe that the ice has been broken and that the security and intelligence agencies understand they can speak more openly about their work without betraying state secrets or compromising national security. The greater the transparency, the less sceptical and cynical the public will be.

It is in this context of transparency that the Commissioner's office organizes periodic luncheon meetings with outside experts in the fields of national security and privacy. This facilitates greater understanding on their part of how we go about our work, and we in turn learn about their perspectives and interests.

Review bodies working cooperatively

My office and the Security Intelligence Review Committee (SIRC) have similar functions but are subject to different legislation. CSEC and CSIS also have different legislation but their respective laws authorize cooperation between them, whereas the legislation governing my office and SIRC does not contain similar provisions. This means that where CSEC and CSIS cooperate and conduct joint activities, my office and SIRC do not have an equivalent authority to conduct joint reviews. Nonetheless, I believe a certain amount of collaboration among review bodies is possible under existing legislation. For example, where I have no mandate to follow-up, I may refer questions to SIRC that concern CSIS. Activities beyond this, such as the sharing of special operational information of the agencies, may require the intervention and approval of Cabinet, and possibly also legislative change. Ideally, the law should authorize, even encourage, such cooperation.

The creation of an over-arching structure that would group existing review bodies under a single umbrella, proposed in a past commission of inquiry report, does not strike me as a sensible solution at this point. Before we create an additional super-bureaucracy, with the associated burden and costs, we may be better advised to optimize existing review bodies and facilitate their collaboration.

Another form of cooperation among security and intelligence review bodies has occurred over the past few years. My office has provided an introductory training course for new employees of security and intelligence review bodies, to explain various review methods and to contribute to the development of more rigorous review practices.

Information sharing with international partners

The growth of international cooperation in the intelligence field has important implications for privacy. We want to ensure that the foreign countries and organizations with which Canada exchanges information protect privacy with as much rigour as Canada exercises. This is not an easy task. On the one hand, nations are sovereign and do not appreciate interference in their internal affairs, particularly not in the area of security. On the other hand, review bodies and mechanisms vary from country to country. In the absence of international intelligence review standards, I believe the best guarantee of the protection of the privacy of Canadians in information exchanged with international partners lies in promoting and ensuring strong and independent review bodies in those countries. We are, in fact, already doing this to some extent.

For the past 15 years, the review bodies of a dozen countries, including members of the "Five-Eyes" countries (Canada, the United States, the United Kingdom, Australia and New Zealand), have attended a biennial conference. These meetings have been a source of rewarding exchanges and new inspiration. The sharing of perspectives and best practices is a stimulating and enriching experience. As well, countries for which independent intelligence review is in its early stages may be invited to attend the conferences as observers and gain knowledge about what is happening elsewhere. Canada hosted this conference in May 2012.

On the bilateral level, my office meets with representatives of foreign review bodies and oversight committees. This past year, for example, I met with members of a delegation of French parliamentarians seeking information on the nature and methodology of Canadian review bodies. I have also met with members of the Belgian Standing Intelligence Agencies Review Committee and the British Intelligence and Security Committee. It is my wish that these kinds of beneficial meetings occur more frequently.

Cyber security and cyber attacks

One can no longer talk about security without mentioning cyber threats. Barely a week goes by without headlines dealing with the risk of breaches of public and private computer systems. CSEC, by its very mandate, is called on to play a leadership role in protecting electronic information and information infrastructures of importance to the Government of Canada. CSEC may also lend its experience to assist Public Safety Canada in its role of helping to protect critical infrastructure that may involve the private sector.

It is unavoidable that CSEC may unintentionally intercept the private communications of Canadians while conducting certain information technology (IT) security activities. For this reason, in recent years, the Commissioner's office has increased its vigilance in this area, completing a number of reviews, while others have been initiated; I have no doubt that my successor will continue this work.

Proposals for legislative changes to the *National Defence Act*

I started my mandate with the expectation that the legislative amendments to the *National Defence Act* proposed by my predecessors would soon be introduced in Parliament, but this has yet to happen. I am deeply disappointed at the lack of action by the government, which is no longer in a minority situation, to address the ambiguities identified by my predecessors and myself. These amendments — as I have said many times before — would improve the provisions that were hastily

enacted in the aftermath of September 11, 2001. The proposals to address the issues raised by Commissioners should not, in my opinion, be controversial.

The independence of the Office of the CSE Commissioner

The office attained its institutional and financial independence just over five years ago when it received its own funding approved by Parliament, and was no longer part of the budget of the Department of National Defence. To emphasize this independence, 2011 marked the first time the Commissioner issued his own news release to highlight the tabling in Parliament of his annual report by the Minister of National Defence. Financial independence, however, does have its drawbacks. As a result of having its own appropriation, the Commissioner's office, a micro-agency with a budget of roughly two million dollars, is subject to the same accounting and reporting requirements as all departments, each with their individual budgets, some into the billions. To my mind, this is an example of excessive bureaucracy that has resulted in a significant level of reporting that is of limited value to both the office and its stakeholders.

MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

My mandate under the *National Defence Act* consists of three key functions:

1. **reviewing CSEC activities** to determine whether they comply with the law;

2. **conducting investigations** I deem necessary in response to complaints about CSEC; and

3. **informing the Minister** of National Defence (who is accountable to Parliament for CSEC) and the Attorney General of Canada of any CSEC activities that I believe may not be in compliance with the law.

Under the *Security of Information Act*, I also have a mandate to receive information from persons who are permanently bound to secrecy if they believe it is in the public interest to release special operational information of CSEC. (More information on the Commissioner's responsibilities for public interest defence is available on the office's website.)

CSEC's mandate

When the *Anti-terrorism Act* came into effect on December 24, 2001, it added Part V.1 to the *National Defence Act*, and set out CSEC's three-part mandate:

- part (a) authorizes CSEC to acquire and use foreign signals intelligence in accordance with the Government of Canada's intelligence priorities;
- part (b) authorizes CSEC to help protect electronic information and information infrastructures of importance to the Government of Canada; and
- part (c) authorizes CSEC to provide technical and operational assistance to federal law enforcement and security agencies, including helping them obtain and understand communications collected under those agencies' own lawful authorities.

Reviewing CSEC activities

My mandate to review CSEC activities relates to CSEC collecting foreign signals intelligence, protecting electronic information and information infrastructures of importance to the Government of Canada, and assisting federal law enforcement and security agencies.

The purpose of my review mandate is:

- to determine whether the activities conducted by CSEC under ministerial authorization are, in fact, those authorized by the Minister of National Defence, and to verify that the conditions for authorization required by the *National Defence Act* are met;
- to determine whether CSEC complies with the law and, if I believe that it may not be complying, to report this to the Minister of National Defence and to the Attorney General of Canada;
- to verify that CSEC does not direct its foreign signals intelligence and IT security activities at Canadians; and
- to promote the development and effective application of satisfactory measures to protect the privacy of Canadians in all the activities CSEC undertakes.

Protection of Canadians

CSEC is prohibited by law from directing its foreign signals intelligence collection and IT security activities at Canadians — wherever they might be in the world — or at any person in Canada.

Ministerial authorizations

The *National Defence Act* allows the Minister of National Defence to give CSEC written ministerial authorization to unintentionally intercept private communications while collecting foreign signals intelligence or

while protecting computer systems of the Government of Canada from mischief, unauthorized use or interference. In each case, the law specifies the conditions under which a ministerial authorization can be issued. Ministerial authorizations relate to an activity or class of activities specified in the authorizations — that is, to a specific method of acquiring foreign signals intelligence or of protecting computer systems (the how); however the authorizations do not relate to a specific individual or subject (the whom or the what). The law also directs the CSE Commissioner to review activities carried out under a ministerial authorization and to report annually to the Minister on the review. (More information on ministerial authorizations as well as on the authorities for and limitations on CSEC activities are available on the office's website.)

Selection of activities for review

I use a risk-based and preventative approach to my reviews. I prioritize CSEC activities where risk is greatest for potential non-compliance with the law, including for risks to the privacy of Canadians, by considering, among other factors:

- the controls placed by CSEC on the activity to ensure compliance with legal, ministerial and policy requirements;
- whether the activity does, or has the potential to, involve private communications or information about Canadians;
- whether the activity is new, has changed significantly, or has had a lengthy period elapse since its last in-depth review;
- whether there have been significant changes to the authorities or technologies relating to the activity;
- whether Commissioners have made findings or recommendations relating to the activity that require follow-up; and
- issues arising in the public domain.

Information about Canadians: any personal information (as described in the *Privacy Act*) about a Canadian, or business information about a Canadian corporation.

Review methodology and criteria

My reviews of activities are *ex post*, that is, of activities that have occurred in the past. However, reviews always include an examination of CSEC's *ex ante* reasons for conducting the activities — to confirm that CSEC's justifications for the activities are lawful and within CSEC's mandate. In conducting a review, my office examines CSEC's hard-copy and electronic information and records, as well as CSEC's policies and procedures and legal advice received from Justice Canada. My employees request briefings and demonstrations of specific activities, interview CSEC managers and employees, and observe CSEC operators and analysts first hand to verify how they conduct their work. My employees test information obtained against the contents of CSEC's systems and databases.

Each review includes an assessment of CSEC activities against a standard set of criteria, described below, consisting of legal requirements, ministerial requirements, and policies and procedures. Each review may have additional criteria added, as appropriate.

Legal requirements: I expect CSEC to conduct its activities in accordance with the *National Defence Act*, the *Canadian Charter of Rights and Freedoms*, the *Privacy Act*, the *Criminal Code*, and any other relevant legislation, and in accordance with Justice Canada advice.

Ministerial requirements: I expect CSEC to conduct its activities in accordance with ministerial direction, following all requirements and limitations set out in a ministerial authorization or directive.

Policies and procedures: I expect CSEC to have appropriate policies and procedures in place to guide its activities and to provide sufficient direction on legal and ministerial requirements including the protection of the privacy of Canadians. I expect CSEC employees to be knowledgeable about and comply with policies and procedures. I also expect CSEC to have an effective compliance validation framework and activities to ensure the integrity of operational activities is maintained, including appropriately accounting for important decisions and information relating to compliance and the protection of the privacy of Canadians.

My classified review reports document CSEC activities and practices and contain findings relating to the above-noted criteria. These reports may also disclose the nature and significance of deviations from the criteria. In some cases, I make recommendations to the Minister that are aimed at correcting discrepancies between CSEC activities and the expectations established by the review criteria.

The logic model in **Annex A** provides a flow chart of the review program (p. 41).

Horizontal reviews

Horizontal reviews examine processes common to all CSEC foreign signals intelligence collection methods or to IT security activities. For example, the processes by which CSEC:

- identifies, selects and directs its activities at foreign entities of intelligence interest located outside Canada or at threats to Government of Canada computer systems;
- uses, shares, reports, retains or disposes of intercepted information; or
- takes measures to protect private communications intercepted unintentionally and to protect information about Canadians.

Conducting investigations

My mandate includes undertaking any investigation I deem necessary in response to a written complaint — for example to determine whether CSEC has engaged, or is engaging, in unlawful activity or is not taking sufficient measures to protect the privacy of Canadians. (More information on the Commissioner's responsibilities for conducting investigations into complaints is available on the office's website.)

Informing the Minister

Under my mandate to keep the Minister of National Defence informed, I:

- forward the results of my reviews, in classified reports, to the Minister; and
- submit an unclassified report to the Minister on my activities each year, which the Minister must then table in Parliament. This is the 17th annual report.

While it is my primary duty to report any non-compliance by CSEC, a necessary element of my mandate also includes informing the Minister of any activities that I believe might present, or have the potential to present, a risk of non-compliance, such as an unlawful interception of a private communication or other invasion of the privacy of a Canadian. A number of my reports have included recommendations aimed at prevention. It is a goal of the Commissioner's office to strengthen CSEC practices that contribute to compliance and incorporate measures that protect the privacy of Canadians.

Independence

While I submit my reports to the Minister of National Defence, who is responsible for CSEC, my office is completely independent and receives its own funding from Parliament. My mandate is supported by the powers I have under the *Inquiries Act*, including the power of subpoena, to ensure access to all CSEC information and employees.

CSE Commissioner

The Commissioner is an independent statutory officer and is not subject to general direction from the Prime Minister, the Minister of National Defence or any other ministers on how to carry out his mandate. The Commissioner assists the Government of Canada in its control of CSEC by providing advice to the Minister to support the Minister's decision making and accountability for CSEC. The Commissioner's classified reports to the Minister and unclassified annual report, through the Minister to Parliament and the public, state whether CSEC has acted lawfully and the extent to which it protected the privacy of Canadians in the conduct of its activities.

Annex B contains the text of the relevant sections of the *National Defence Act* and the *Security of Information Act* relating to my role and mandate as CSE Commissioner (p. 43). (Information on the history of the Office of the CSE Commissioner is available on the office's website.)

COMMISSIONER'S OFFICE

Last year, work was completed on the expansion of the physical space of the office, to provide sufficient accommodation for existing functions, and for additional responsibilities resulting from the office receiving its own appropriation from Parliament. The expansion will allow me to hire two additional review officers to enable adequate review of CSEC, which has experienced significant growth. I have been supported in my work by a staff of eight, together with a number of subject-matter experts, as required. In 2012–2013, my office's expenditures were $2,285,718, which is within the overall funding approved by Parliament.

Annex C provides the 2012–2013 Statement of Expenditures for the Office of the CSE Commissioner (p. 47).

IMPACT OF COMMISSIONERS' RECOMMENDATIONS

Since 1997, my predecessors and I have submitted to the Minister of National Defence 74 classified review reports. In total, the reports contained 138 recommendations. CSEC has accepted and implemented or is working to address 92 percent (127 out of 138) of these recommendations.

Commissioners monitor how CSEC addresses recommendations and responds to negative findings as well as areas for follow-up identified in past reviews. This past year, CSEC advised my office that work had been completed in response to 14 past recommendations. Notably, CSEC implemented recommendations by:

- providing support to the Minister of National Defence to update certain ministerial directives;
- updating general memoranda of understanding for the exchange of information and operational cooperation with CSIS and Foreign Affairs and International Trade Canada;
- committing to report to the Minister of National Defence certain information (that cannot be publicly identified for security reasons), as a measure to protect the privacy of Canadians and to support the Minister in his accountability for CSEC;
- promulgating a revised policy for operational assistance to law enforcement and security agencies under part (c) of CSEC's mandate, including guidance on the retention and disposition of records relating to any assistance;
- promulgating a revised procedure that defines risk and risk mitigation for certain foreign signals intelligence collection activities as well as adopting a risk management framework for the planning and approval of these activities; and

- launching a new secure system with other government departments and agencies for handling and tracking requests for and disclosures of suppressed Canadian identity information.

These actions by CSEC demonstrate that review works. The Commissioner's office will examine the impact of these enhancements on compliance and privacy protection in future reviews. In addition, the Commissioner's office is monitoring six active recommendations that CSEC is working to address. The Minister's responses to two recommendations of this year were not received by the time this report was completed.

The office's website provides a complete list of the 74 classified review reports submitted to the Minister of National Defence.

OVERVIEW OF 2012–2013 FINDINGS AND RECOMMENDATIONS

During the 2012–2013 reporting year, I submitted six reports to the Minister of National Defence on my review of CSEC activities.

These reviews were conducted under two areas of my mandate:

- ensuring CSEC activities are in compliance with the law — as set out in paragraph 273.63(2)(*a*) of the *National Defence Act*; and
- ensuring CSEC activities under a ministerial authorization are authorized — as set out in subsection 273.65(8) of the *National Defence Act*.

The results

Each year, I provide an overall statement on my findings about the lawfulness of CSEC activities. With the exception of one review described below — in which I was unable to reach a definitive conclusion about compliance or non-compliance with the law for certain CSEC foreign signals intelligence activities — all of the activities of CSEC reviewed this past year complied with the law.

As well, this year, I made four recommendations to promote compliance with the law and to strengthen privacy protection. The recommendations, which are described in the following review summaries, relate to reinforcing policy guidance and expanding an existing practice on privacy protection to other circumstances, as well as providing the Federal Court of Canada with certain additional evidence about the nature and extent of the assistance CSEC may provide to CSIS.

Additionally, I forwarded to the Chair of SIRC, for information, certain general points relating to CSIS that arose out of the recommendations I made and that SIRC may wish to examine as it deems appropriate. This demonstrates how existing review bodies can, in the spirit of the recommendations of the commission of inquiry led by the Honourable Justice Dennis O'Connor, collaborate under existing legislation in the conduct of reviews of activities involving more than one security and intelligence agency.

Two reviews this year — the review of certain foreign signals intelligence activities and the review of CSEC assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the *Canadian Security Intelligence Service Act* (*CSIS Act*) — identified the absence of certain historical information in a CSEC system and database relating to foreign signals intelligence collection. This system and database support the process by which CSEC determines that entities of foreign intelligence interest are indeed foreign and located

outside of Canada, as required by the *National Defence Act*. The absence of the information limited my ability to assess the lawfulness of the CSEC activities in question, and could also affect review of other activities of CSEC. Due to the seriousness of this development, I directed my employees to conduct an in-depth examination of the issue to determine the implications and advise on a resolution. This issue added to the time required to complete these two reviews. It is encouraging that CSEC has already taken action and continues to do so to ensure the availability of information that is required for accountability and to demonstrate compliance with the law. The Commissioner's office will monitor developments.

In last year's annual report, I expressed frustration about a reduction in CSEC support to my office resulting in excessive delays in being able to proceed with some reviews. CSEC has taken steps to correct this situation and I am optimistic that these will result in a productive year ahead.

HIGHLIGHTS OF THE SIX REVIEWS SUBMITTED TO THE MINISTER IN 2012–2013

1. Review of certain foreign signals intelligence activities

Background

I examined CSEC's acquisition, use and exchange of information relating to certain foreign intelligence activities that occurred a number of years ago.

Findings and recommendations

I had no concern with respect to the majority of the CSEC activities reviewed. However, a small number of records suggested the possibility that some activities may have been directed at Canadians, contrary to law. A number of CSEC records relating to these activities were unclear or incomplete. After in-depth and lengthy review, I was unable to reach a definitive conclusion about compliance or non-compliance with the law.

In the process of review, I found that a number of CSEC records relating to exchanges of information with CSIS were sometimes unclear, which led me to recommend that CSEC promulgate policy guidance respecting how to clearly and consistently communicate with its partners about what entity the activities are being directed at. As well, I recommended that CSEC ensure that its foreign intelligence analysts are knowledgeable about and follow existing policy guidance, introduced since the period under review, respecting their responsibilities for determining the foreign status of an entity and the justifications for directing activities at that entity. Following the completion of my review, I forwarded to the Chair of SIRC, for information, certain general points relating to CSIS that arose out of the recommendations I made.

At my direction, my office has started a review of other more recent foreign intelligence activities that includes follow-up on matters raised in this review, and will seek to determine whether developments in CSEC policies and procedures since the period under review have led to an improvement in the clarity of language in CSEC information exchanges with CSIS.

Conclusion

As of the end of the 2012–2013 reporting period, March 31, 2013, I am awaiting the Minister's response to the two recommendations. The responses will be noted in next year's annual report.

2. CSEC assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the *CSIS Act*

Background

In 2007, CSIS sought from the Federal Court of Canada a warrant to assist in the investigation of threat-related activities that, it was believed, individuals would engage in while travelling outside of Canada. The Honourable Justice Edmond Blanchard held that the Court lacked the jurisdiction to authorize intrusive investigative activities by CSIS employees *outside of Canada* (*Re CSIS Act*, 2008 FC 301).

In 2009, in *X(Re)*, 2009 FC 1058, the Court was asked to revisit the question of jurisdiction and to distinguish Justice Blanchard's reasoning on the basis of a more complete description of the facts relating to the activities necessary to permit the interception and a different legal argument concerning how the method of interception was relevant to the jurisdiction of the Court. The Honourable Justice Richard Mosley was satisfied that there were sufficient factual and legal grounds to distinguish the application from that which was before Justice Blanchard and he issued the first warrant permitting CSIS to intercept the

communications of Canadians located outside Canada using the interception capabilities of CSEC. The application was supported by the affidavit evidence of an employee of CSEC that described the agency's interception capabilities and how communications would be intercepted *from within Canada.*

Paragraph 273.64(1)(*c*) of the *National Defence Act* authorizes CSEC to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. This assistance includes CSEC supporting CSIS with the interception of Canadians' communications if CSIS has a judicially authorized warrant issued under section 21 of the *CSIS Act*. Pursuant to subsection 273.64(3) of the *National Defence Act*, CSEC is subject to any limitations imposed by law on the agency to which it is providing assistance — for example, any conditions imposed by a judge in a warrant. When CSEC provides operational assistance to CSIS, CSEC becomes the agent of CSIS. CSIS is *de jure* the owner of the information and the intercepted communications relating to the subject of the warrant.

In *X(Re)*, Justice Mosley stated:

> Canada has given CSE[C] a mandate to collect foreign intelligence including information from communications and information technology systems and networks abroad. It [CSEC] is restricted as a matter of legislative policy from directing its activities against Canadians or at any person within Canada, but it is not constrained from providing assistance to security and law enforcement agencies acting under lawful authority such as a judicial warrant. CSIS is authorized to collect threat-related information about Canadian persons and others and, as discussed above, is not subject to territorial limitation.
>
> Where the statutory prerequisites of a warrant are met, including prior judicial review, reasonable grounds and particularization of the targets, the collection of the information by CSIS with

> CSE[C] assistance, as proposed, falls within the legislative scheme approved by Parliament and does not offend the *Charter*. (*X(Re)* at paragraphs 75-76)

The objectives of my review were to acquire detailed knowledge of and to document CSEC's assistance to CSIS and to assess whether CSEC activities complied with the law, including with the terms of the warrants issued to CSIS, and any privacy protections found therein. CSEC's assistance to CSIS under the warrants may include use of Canadian identity information and the interception of the communications of Canadians. CSEC's collection, as defined in the warrant, may impact on the privacy of Canadians.

I examined CSEC assistance to CSIS in support of a number of the first warrants of this kind relating to counter-terrorism. Specifically, as part of assessing compliance with the law and privacy protection, for the warrants examined, I verified that:

- CSEC had a copy of the warrant and had clear and sufficient information about the assistance sought by CSIS;
- the communications targeted by CSEC for CSIS were only those communications referred to in the warrants;
- the communications were not targeted before the warrants came into force and were no longer targeted once the warrants expired;
- CSEC targeted the subjects of the warrants only while they were believed to be outside Canada;
- CSEC targeted only the types of communications and information that were authorized in the warrants to be intercepted or obtained; and
- CSEC complied with any other limitations imposed by law on CSIS, for example, any conditions in the warrants.

Findings and recommendations

During the period under review, CSEC responded appropriately to two related privacy incidents it identified involving the unintentional release of Canadian identity information of some of the subjects of the warrants. In fact, CSEC has already clarified appropriate internal processes for the conduct of certain activities and reminded its employees of their information stewardship responsibilities. This should help prevent similar incidents.

I questioned CSEC about another incident involving the interception of communications for CSIS for a small number of days after a particular warrant had expired. I accepted CSEC's explanation for this incident, which was that it resulted from unintentional human error. CSEC also confirmed that these intercepted communications were destroyed and that CSIS did not receive them. I am satisfied that CSEC documented this incident and reminded its employees of proper process to help prevent similar errors.

During the period under review, operational policies and procedures of general application to CSEC's assistance in support of these warrants and related activities were in place and provided direction to CSEC employees respecting compliance with the law and the protection of the privacy of Canadians. Subsequent to the period under review, CSEC issued specific guidance for the conduct of this assistance and activities. Generally, CSEC employees interviewed were well aware of the policies and procedures and demonstrated knowledge of their respective responsibilities. Interviews with CSEC managers, team leaders and other employees showed that managers routinely monitored the assistance and related activities for compliance with governing authorities.

In addition to a detailed examination of CSEC activities under the warrants, I considered and consulted my independent counsel, who is also a privacy law expert, on general questions of law relating to this subject. I made two recommendations to the Minister to help ensure

CSEC assistance to CSIS is consistent with the authorities and limitations of the warrants, and to enhance the measures in place to protect the privacy of Canadians. Specifically, I recommended that:

1. CSEC discuss with CSIS the expansion of an existing practice to protect privacy to other circumstances; and

2. CSEC advise CSIS to provide the Federal Court of Canada with certain additional evidence about the nature and extent of the assistance CSEC may provide to CSIS.

I found that CSEC practices relating to its assistance to CSIS and related activities were consistent with the general requirements in the "Accountability Framework" and "Privacy of Canadians" ministerial directives to CSEC, specifically to comply with the law and to take measures to ensure that information was lawfully obtained and handled in a manner consistent with the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*.

Conclusion

While I made two recommendations to the Minister to help ensure CSEC assistance to CSIS is consistent with the law and to enhance privacy protection, I concluded that CSEC conducted its activities in accordance with the law and ministerial direction, and in a manner that included measures to protect the privacy of Canadians. The Minister accepted and CSEC has addressed the recommendations.

Following the completion of my review, I forwarded to the SIRC Chair, for information, certain general points relating to CSIS that arose out of the two recommendations I made and that SIRC may wish to examine as it deems appropriate. Subsequently, CSEC advised me that it raised the recommendations — which relate to matters that are controlled by CSIS, or require agreement from CSIS — with CSIS.

3. Review of CSEC IT security activities not conducted under a ministerial authorization

Background

The *National Defence Act* mandates CSEC to provide advice, guidance and services to Government of Canada departments and agencies as well as to other owners of IT systems to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada (paragraph 273.64(1)(*b*)).

During the period under review, the Government of Canada reorganized its cyber defence efforts. CSEC became the primary point of contact for cyber incidents faced by Government of Canada departments and agencies. Public Safety Canada is the primary point of contact for cyber incidents affecting non-Government of Canada critical infrastructure sectors. A further distinction is that CSEC is responsible for sophisticated cyber threats, such as those stemming from foreign state actors, while Public Safety Canada responds to less sophisticated threats, for example, those relating to known vulnerabilities in commercially available computer software.

I examined certain IT security activities conducted by CSEC to detect, analyse and mitigate cyber threats. CSEC does not undertake these activities under a ministerial authorization as it does not intercept communications. Rather, CSEC uses information acquired by the system owners — under their *Criminal Code* authorities and, for Government of Canada system owners, also under their *Financial Administration Act* authorities — and disclosed to CSEC. These authorities permit the interception of private communications by authorized persons when the interception is reasonably necessary to protect computer systems from mischief and unauthorized use.

The objectives of my review were to assess whether CSEC complied with the law and the extent to which CSEC protected the privacy of Canadians in carrying out the activities. In addition to acquiring detailed knowledge about the activities, I examined:

- the legislative and policy framework for the activities;
- CSEC organizational changes;
- technologies, databases and systems used for the activities;
- the amount and treatment of private communications and Canadian identity information acquired by the activities as well as a sample of those private communications and Canadian identity information used by CSEC; and
- agreements in place with Government of Canada departments and agencies.

Private Communication: "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it" (section 183 of the *Criminal Code*).

I examined activities conducted between April 1, 2009, and March 31, 2011, including a more detailed examination of activities and associated reporting for a number of the departments and agencies assisted by CSEC during that time. Additionally, records were examined to verify that system owner information retained by CSEC was done so under an appropriate legal authority. My review also included an examination of CSEC's responses to areas for follow-up identified in a 2009 study by former Commissioner Gonthier.

Findings

I found that CSEC conducted its activities in accordance with the law and ministerial direction and I had no questions about the reporting and retained information examined.

I suggested that CSEC could enhanse its ability to demonstrate that it has measures to protect the privacy of Canadians by recording the return or deletion of irrelevant information acquired by a system owner and shared with CSEC. Notwithstanding this suggestion, I found that these IT security activities contained satisfactory measures to protect the privacy of Canadians.

During the period under review, operational policies and procedures of general application were in place to provide general direction respecting compliance with the law and the protection of privacy of Canadians. However, there was no specific operational guidance in place for these activities. It is a positive development that, subsequent to the period under review, CSEC issued a specific policy for the conduct of these activities.

Some CSEC employees who were interviewed were unable to cite certain policies, but were aware of the rules governing their activities. In addition, CSEC managers who were interviewed routinely and closely monitored the activities to ensure that their employees complied with governing authorities. Based on the records examined, the answers provided to questions during interviews and CSEC's policy compliance validation activities, the activities reviewed complied with relevant policies and procedures.

Conclusion

My review report contained no recommendations. However, regular in-depth reviews will continue to be conducted of IT security activities not conducted under a ministerial authorization to verify compliance with the law, and the extent to which CSEC protects the privacy of Canadians in carrying out the activities.

4. Review of CSEC's 2010–2011 and 2011–2012 foreign signals intelligence ministerial authorizations

Background

Subsection 273.65(8) of the *National Defence Act* requires the Commissioner to review CSEC activities carried out under ministerial authorizations "to ensure they are authorized and report annually to the Minister [of National Defence] on the review." A regular combined review of the foreign signals intelligence ministerial authorizations is one way that Commissioners fulfill this part of their mandate. This year's review covered two fiscal years: I examined the five foreign signals intelligence ministerial authorizations in effect from December 1, 2010, to November 30, 2011, relating to five activities or classes of activities, as well as the six foreign signals intelligence ministerial authorizations in effect from December 1, 2011, to November 30, 2012, relating to six activities or classes of activities. The purpose of this review was to:

1. ensure that the activities conducted under the ministerial authorizations were authorized and that the Minister was satisfied that the four conditions for authorization required by paragraphs 273.65(2)(*a*) to (*d*) of the *National Defence Act* were met;

2. identify any significant changes to the ministerial authorization documents themselves or to CSEC's activities described in the ministerial authorizations;

3. assess the impact, if any, of these changes on the risk of non-compliance and on the risk to privacy, and, as a result, identify any subjects requiring follow-up review; and

4. examine, for compliance with the law, a sample of my choosing of any resulting private communications unintentionally intercepted by CSEC while conducting foreign signals intelligence collection activities under the ministerial authorizations.

Private communications

The Commissioner monitors the number of private communications unintentionally intercepted and verifies how CSEC treated and used these communications. The Commissioner is able to review all of the private communications that CSEC uses and retains.

Findings

I found that the activities conducted under the 2010–2011 and the 2011–2012 foreign signals intelligence ministerial authorizations were authorized.

For each of the 11 foreign signals intelligence collection activities, I examined certain key information relating to interception and to the privacy of Canadians, to permit comparison of the activities and to identify any significant changes or trends over time. I found no significant changes to the scope or operation of any of the activities to require a follow-up in-depth review of specific activities. The 2010–2011 and 2011–2012 foreign signals intelligence ministerial authorizations did not contain any significant changes from the previous year and CSEC did not make any significant changes to the technologies used for these activities.

Changes made by CSEC in 2010–2011 and in 2011–2012 to its operational policies for foreign signals intelligence collection activities clarified authorities and practices and enhanced the protection of the privacy of Canadians.

I also reviewed a sample of unintentionally intercepted private communications that CSEC recognized and retained, and that CSEC did not use in its reports. I found that in both 2010–2011 and 2011–2012, CSEC retained only those private communications essential to international affairs, defence or security, as required by paragraph 273.65(2)(*d*) of the *National Defence Act*. Again this year, the proportion of these communications remained very small and CSEC destroyed most of them. In addition, a new tool is being developed that will assist CSEC analysts in identifying intercepted communications that might be private communications. The Commissioner's office will examine the impact of this new tool on compliance and privacy protection in a future review.

In last year's report, I indicated that certain information about intercepted communications involving CSEC's international partners was not readily available. It is positive that, while not a requirement in the ministerial authorizations, CSEC has recognized the importance of reporting this information to the Minister. The Commissioner's office will monitor developments.

It is also a positive development that, while not a requirement of a particular ministerial authorization, CSEC has agreed to report to the Minister certain information relating to privacy. This measure to protect the privacy of Canadians will support the Minister in his accountability for CSEC. It also satisfies an outstanding recommendation I made in 2010–2011. The Minister had initially supported CSEC's rejection of this recommendation. However, after further examination, I maintained my recommendation and so informed the Minister. CSEC reconsidered its initial position and advised the Minister that it would undertake to implement the recommendation.

Conclusion

I made no recommendations.

5. Annual review of a sample of disclosures of Canadian identity information to Government of Canada clients

Background

Canadian identity information may be included in CSEC's foreign signals intelligence reports if it is required to understand or use the foreign intelligence. However, any information that identifies a Canadian must be suppressed in the reports — that is, replaced by a generic reference such as "a named Canadian." When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC must verify that the requesting client has both the authority and operational justification for obtaining the Canadian identity information. Only then may CSEC provide that information.

My officials selected and examined a sample of approximately 20 percent of the total number of disclosures by CSEC to Government of Canada agencies or departments during the period October 2011 to June 2012. The sample included disclosures made to all of the departments that had requested Canadian identity information during the period under review. My officials examined: the requests documenting the clients' authority and justification for obtaining the Canadian identity information; associated CSEC foreign signals intelligence reports; and the actual disclosures of Canadian identity information.

Findings

Based on my assessment of the information reviewed and the interviews conducted, CSEC conducted its disclosure activities in compliance with the law. Operational policies and procedures are in place and provide sufficient direction to CSEC employees respecting the protection of the privacy of Canadians. CSEC employees were knowledgeable about, and acted in accordance with, the policies and procedures.

In addition, in response to a recommendation made by former Commissioner Cory in his 2010 report, in 2012, CSEC started using a new on-line secure system to process requests for and disclosures of Canadian identity information. CSEC provided my employees with a demonstration of the system, which is currently used with CSEC's principal clients. CSEC intends to extend its use to other partners starting in the coming fiscal year. According to CSEC, the system has improved the timeliness of responses and resulted in better service to its clients. It enhances accountability by improving the tracking and retrieval of requests for and disclosures of Canadian identity information and it contains a number of features to help ensure the protection of the privacy of Canadians.

Conclusion

My review did not result in any recommendations. CSEC conducted its disclosure activities in a thorough manner; all of the requests reviewed were authorized, justified and well documented.

Should there be an instance of non-compliance in CSEC disclosure of Canadian identity information, the potential impact on the privacy of Canadians could be significant. For this reason, annual reviews of a sample of disclosures will continue. Next year's sample will include a detailed examination of the use of the new system, as well as a sample of disclosures of Canadian identity information to CSEC's international partners.

6. Annual review of incidents and procedural errors identified by CSEC in 2012 that affected or had the potential to affect the privacy of Canadians and measures taken by CSEC to address them

Background

CSEC maintains a central file describing any operational incidents that did or could have an impact on the privacy of Canadians. CSEC records in this file any incidents it identifies that put at risk the privacy of a Canadian in a manner that runs counter to or is not provided for in its operational policies. CSEC policy requires its foreign signals intelligence and IT security employees to report and document privacy incidents in order to demonstrate compliance with legal requirements and CSEC policies, and to prevent further incidents. Incidents could include, for example, the inadvertent inclusion of Canadian identity information in a report, or mistakenly sharing a report with the wrong recipient.

Horizontal and in-depth reviews of CSEC activities include an examination of any privacy incidents and procedural errors relating to the subject under review and, where appropriate, are reported in the summaries of those reviews. My employees are vigilant during reviews about identifying these types of incidents, so we can confirm whether CSEC also identified and addressed them.

The objectives of this annual review are to: acquire knowledge of the incidents and procedural errors in 2012 and associated actions; and inform development of the Commissioner's work plan, by determining if there are any systemic issues or issues about compliance with the law or the protection of the privacy of Canadians that should be the subject of follow-up review. The review of these privacy incidents and procedural errors also assists in evaluating how CSEC monitors and validates that its activities adhere to its operational policies.

Findings

I examined all foreign signals intelligence and IT security privacy incidents and procedural errors recorded by CSEC in calendar year 2012, and the subsequent actions taken by CSEC to correct them.

There was a very small number of procedural errors and I agreed with CSEC's assessment that these occurrences were minor and did not amount to privacy incidents.

Based my review of CSEC's records as well as independent verification by my office of reports in a CSEC database, I am satisfied that CSEC took appropriate corrective actions in response to the small number of privacy incidents it recorded.

I was particularly pleased with certain remedial actions taken by CSEC to prevent future similar privacy incidents. For example, CSEC is now conducting a monthly review of its central file to ensure that all required remedial activities have been completed or are being pursued. As well, CSEC reminded its employees of the requirement to report an incident immediately. CSEC also established a process to send reminders to its employees to make sure that certain information in its systems is up to date and compliant with existing authorities.

Conclusion

My review of the privacy incidents and procedural errors identified by CSEC in 2012 did not result in any recommendations. My review did not reveal any systemic deficiencies or issues that require follow-up review. Annual reviews will continue to be conducted of the privacy incidents and procedural errors identified by CSEC.

COMPLAINTS ABOUT CSEC ACTIVITIES

In 2012–2013, my office was contacted by a number of individuals who were seeking information or expressing concern about CSEC activities. However, the inquiries were assessed as outside of the Commissioner's mandate or as lacking credibility. No complaints about CSEC activities warranted investigation by the Commissioner. (More information on the complaints process is available on the office's website.)

DUTY UNDER THE *SECURITY OF INFORMATION ACT*

I have a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy seeking to defend the release of special operational information — such as certain information relating to CSEC activities — on the grounds that it is in the public interest. No such matters were reported to me in 2012–2013. (More information on the Commissioner's responsibilities under the *Security of Information Act* is available on the office's website.)

ACTIVITIES OF THE COMMISSIONER'S OFFICE

In last year's annual report, in an attempt to clarify misconceptions and to better inform the public about CSEC's and my mandates and activities, I provided more detail than ever before on CSEC's activities, what Commissioners review, how reviews are carried out, and the impact of reviews. Work is ongoing to improve the website, which contains detailed information on the activities of the Commissioner's office. Of course, the Commissioner provides the Minister of National Defence with additional classified information — which cannot be disclosed in this public report or on the website — so that the Minister can be fully aware of the Commissioner's review of CSEC activities. Last year, employees of my office and I also met with a number of academics and other professionals interested in review of security and intelligence agencies to talk about my role and work and their views on effective review. In addition, my office made presentations to five cohorts of new CSEC employees attending

CSEC's foundational learning course, which is a requirement for every new employee. These presentations provide an introduction to what it is I and my office do, how we go about our work, and how it may affect them as CSEC employees.

During the past year, CSEC provided a number of detailed briefings to employees of my office as part of the conduct of reviews. CSEC also provided an overview briefing on recent and important operational, policy and organizational changes and issues. I attended an interactive presentation that demonstrated CSEC's foreign signals intelligence capabilities and response to an incident. The event was very effective in demonstrating how the many different parts of CSEC, many personnel and many different government departments and agencies cooperate, in response to a top Government of Canada priority. I was struck by the knowledge and professionalism of CSEC employees and their evident dedication to their respective responsibilities. In addition, my employees attended CSEC training on foreign signals intelligence activities and on communications security.

Following a conference on security and privacy at the Université de Montréal in October 2011, my office's Executive Director wrote a chapter in a book, *Circulation internationale de l'information et sécurité,* published in late 2012. The chapter was based on his participation in one of the conference panels, describing distinctions between national security and public safety, the role and impact of review, and the integration of technology and privacy protection in national security.

At the beginning of March, the Executive Director delivered a luncheon address at the 15th annual conference organized by the Centre for Military and Strategic Studies at the University of Calgary, with the theme *Global Security: Past, Present and Future*. His address dealt with the role of intelligence review, focussing on four questions: why is review important; how effective can it be and what makes for effective review; what is the view of the intelligence agencies themselves concerning review; and what of the future and some challenges.

WORK PLAN — REVIEWS UNDER WAY AND PLANNED

Commissioners use a risk-based and preventative approach to reviews. A three-year work plan is updated twice a year. Developing the work plan draws on many sources. Two important ones are regular briefings from CSEC on new activities and changes to existing activities, and the Chief of CSEC's classified annual reports to the Minister of National Defence on CSEC's priorities and legal, policy and management issues of significance.

The results of several reviews currently under way are expected to be reported to the Minister of National Defence in the coming year and included in my successor's 2013–2014 annual report. The subjects of these reviews include: CSEC counter-terrorism activities; a follow-up to this year's review of certain foreign signals intelligence activities; CSEC's policy compliance validation framework and activities; and a review of particular signals intelligence collection activities conducted under ministerial authorizations.

In addition, before the end of my term as Commissioner, I will report to the Minister on my ongoing review of CSEC's foreign signals intelligence sharing with its closest international partners — the United States' National Security Agency, the United Kingdom's Government Communications Headquarters, the Australian Defence Signals Directorate and the New Zealand Government Communications Security Bureau. CSEC and its international partners respect each other's laws by pledging not to direct collection activities at one another's citizens' communications. CSEC is prohibited from requesting an international partner to undertake activities that CSEC itself is legally prohibited from conducting. However, CSEC sharing information with its international partners could affect a Canadian; it is in the international sharing of personal information where the risks are higher than for sharing involving domestic partners. My 2011–2012 annual report contained an update on

this review. This year, I continued my in-depth review and consulted my independent counsel on general questions of law relating to this subject.

Some of the reviews planned for 2013–2014, which may carry over to the next year, are: a review of CSEC IT security activities conducted under ministerial authorizations in support of Government of Canada efforts to address cyber threats; a follow-up review of CSEC activities carried out under a ministerial directive for the purposes of identifying new foreign entities believed to be of foreign intelligence interest; and a follow-up review of CSEC efforts to address numerous gaps related to CSEC's dealings with the Canadian Armed Forces, as identified by CSEC internal evaluators. In addition, the office plans to continue the annual reviews of: (1) foreign signals intelligence ministerial authorizations; (2) CSEC disclosures of Canadian identity information; and (3) privacy incidents and procedural errors identified by CSEC and the measures subsequently taken by CSEC to address them. The office will work with my successor to put in place a comprehensive work plan soon after his or her appointment.

IN CLOSING

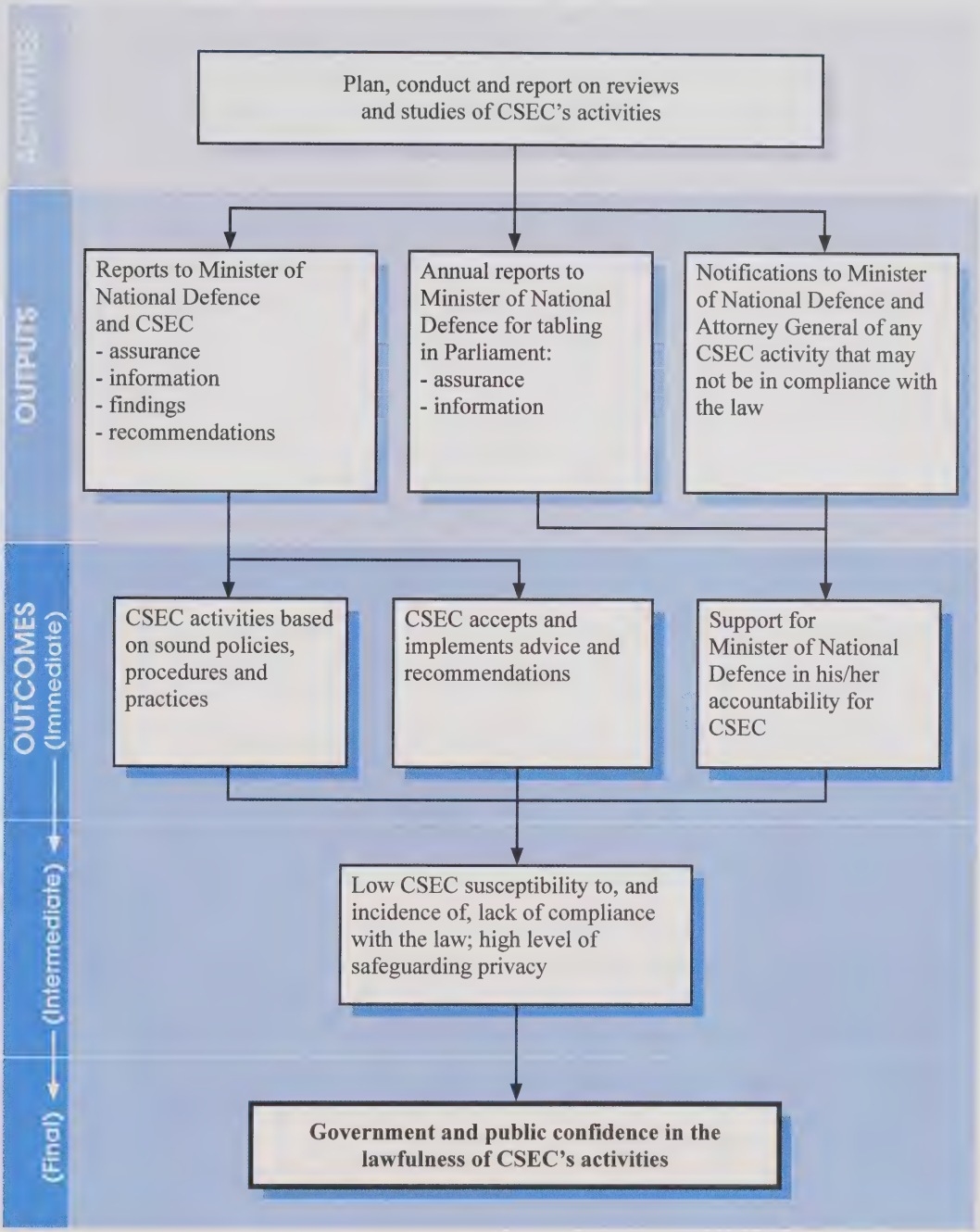
The position of Commissioner is a legislated part of how the government decided, in enacting the *National Defence Act*, to strike a balance between — on the one hand — the Government of Canada's need for foreign signals intelligence and IT security services, and — on the other hand — the need to protect the privacy of Canadians.

The role of the Commissioner and the Commissioner's office is to be sceptical and critical of CSEC activities and it is natural that our respective organizations may sometimes disagree. However, we have a shared objective with CSEC, which is to ensure CSEC complies with the law and protects the privacy of Canadians in the conduct of its activities.

The fulfillment of the Commissioner's mandate rests on the integrity of the office, its ability to effect change at CSEC and inspire confidence in the public that CSEC is under rigorous review.

Finally, I thank the staff of my office, whose dedication, enthusiasm, teamwork, rigour and sense of duty have been nothing short of remarkable these past three years. I can say with pride and confidence that CSEC is truly being watched.

ANNEX A: COMMISSIONER'S OFFICE REVIEW PROGRAM — LOGIC MODEL



ANNEX B: EXCERPTS FROM THE *NATIONAL DEFENCE ACT* AND THE *SECURITY OF INFORMATION ACT* RELATED TO THE COMMISSIONER'S MANDATE

***National Defence Act* — Part V.1**

Appointment of Commissioner

273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

Duties

(2) The duties of the Commissioner are

(*a*) to review the activities of the Establishment to ensure that they are in compliance with the law;

(*b*) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(*c*) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

Annual report

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

Powers of investigation

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

Employment of legal counsel, advisors, etc.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

Directions

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

[...]

Review of authorizations

273.65 (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

Public interest defence

15. (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]

Prior disclosure to authorities necessary

(5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]

(*b*) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

ANNEX C: 2012-2013 STATEMENT OF EXPENDITURES

Standard Object Summary ($)

Salaries and Benefits	907,567
Transportation and Telecommunications	15,412
Information	59,131
Professional and Special Services	305,572
Rentals	217,803
Repairs and Maintenance	1,515
Material and Supplies	10,383
Machinery and Equipment	16,985
Capital Assets, including Leasehold Improvements	751,350
Total	**2,285,718**

ANNEXE C : ÉTAT DES DÉPENSES DE 2012-2013

Sommaire des articles courants (en dollars)

Salaires et avantages sociaux	907 567
Transport et télécommunications	15 412
Information	59 131
Services professionnels et spéciaux	305 572
Locations	217 803
Achat de services de réparation et d'entretien	1 515
Matériels et fournitures	10 383
Machines et équipement	16 985
Immobilisations totales, y compris les améliorations locatives	751 350
Total	**2 285 718**

Loi sur la protection de l'information

Défense d'intérêt public

15. (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public. [...]

Informer les autorités

(5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation qui si la personne s'est conformée aux exigences suivantes : [...]

b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous procureur général du Canada dans un délai raisonnable, elle a informé de la question avec tous les renseignements à l'appui en sa possession, [...]

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui ci, et n'en a pas reçu de réponse dans un délai raisonnable.

Loi sur les enquêtes

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

Assistance

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques, ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions. Il peut fixer avec l'approbation du Conseil du Trésor leur rémunération et leurs frais.

Fonctions du commissaire

(6) Le commissaire exerce les attributions que lui confère la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

Révision

273.65 (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.

ANNEXE B : EXTRAITS DE *LA LOI SUR LA DÉFENSE NATIONALE* ET DE LA *LOI SUR LA PROTECTION DE L'INFORMATION* RELATIFS AU MANDAT DU COMMISSAIRE

***Loi sur la défense nationale* — Partie V.1**

Nomination du commissaire

273.63 (1) Le gouverneur en Conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite [ou] surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

Mandat

(2) Le commissaire a pour mandat :

a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

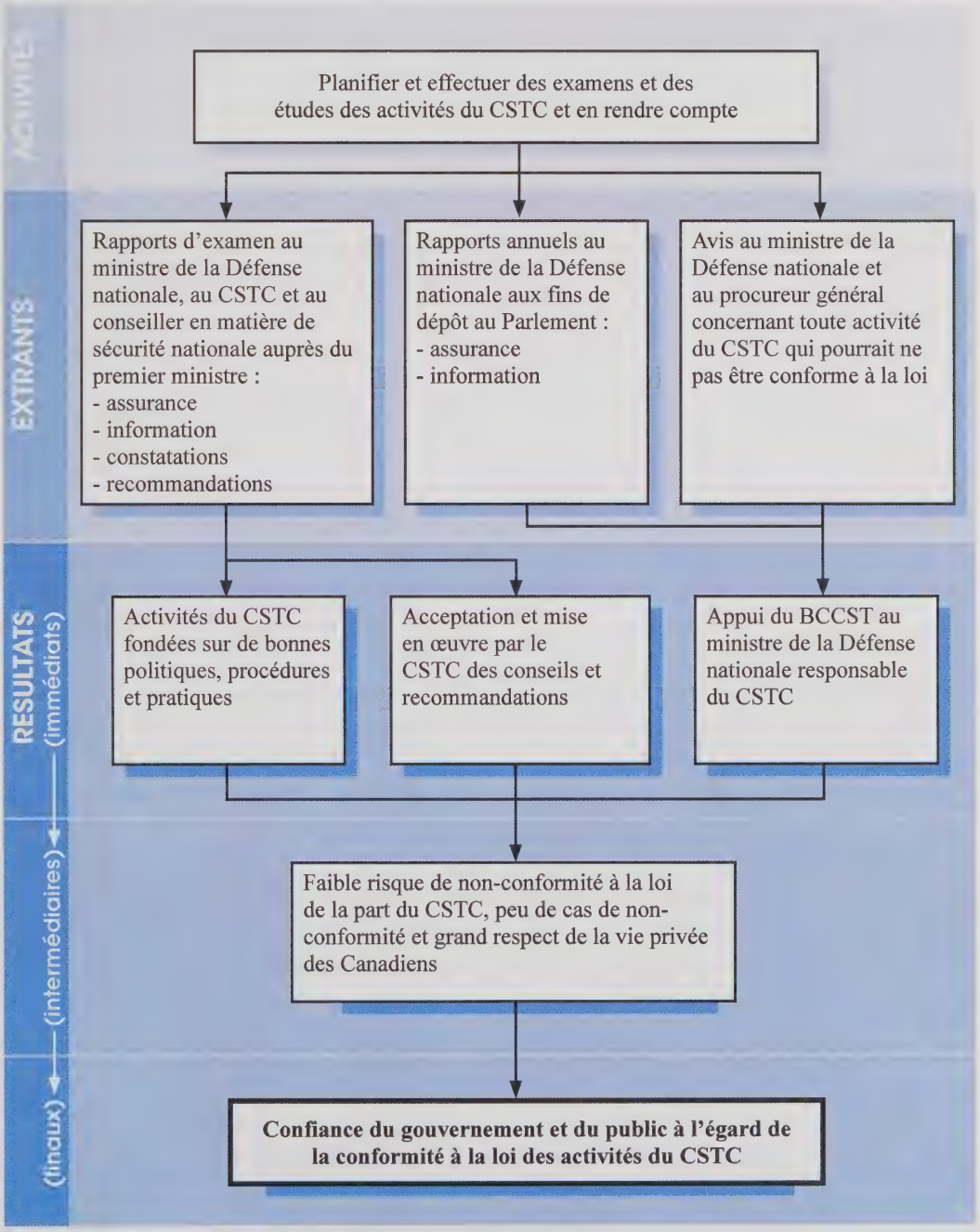
b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

Rapport annuel

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours (90) suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze (15) premiers jours de séance de celle-ci suivant sa réception.

ANNEXE A : PROGRAMME D'EXAMEN DU BUREAU DU COMMISSAIRE – MODÈLE LOGIQUE



électromagnétiques étrangers, 2) de la divulgation par le Centre de renseignements concernant l'identité de Canadiens et 3) des incidents et des erreurs de procédure signalés par le Centre qui ont touché ou auraient pu toucher la vie privée de Canadiens ainsi que des mesures prises par le Centre pour régler le problème. Le Bureau travaillera avec mon successeur à mettre en place un plan de travail exhaustif peu de temps après sa nomination.

EN GUISE DE CONCLUSION

Le poste de commissaire constitue un rouage mis en place par le Parlement, qui témoigne de la façon dont le gouvernement a décidé, en adoptant la *Loi sur la défense nationale,* de trouver un juste équilibre entre, d'une part, la nécessité de déposer de services de renseignements électromagnétiques étrangers et de protection des technologies de l'information du gouvernement du Canada et, d'autre part, la nécessité de protéger la vie privée des Canadiens.

Le rôle du commissaire et de son Bureau est d'examiner avec scepticisme et un esprit critique les activités du Centre. Il est dès lors naturel que nos organisations respectives soient parfois en désaccord. Toutefois, nous avons un objectif commun : celui de faire en sorte que le Centre se conforme à la loi et protège la vie privée des Canadiens dans la conduite de ses activités.

Le succès du mandat du commissaire repose sur l'intégrité de son Bureau et sur sa capacité d'amener le Centre à effectuer les changements requis, ainsi que sur sa capacité de gagner la confiance du public en lui montrant que le Centre fait l'objet d'une surveillance rigoureuse.

Enfin, je remercie le personnel de mon Bureau dont le dévouement, l'enthousiasme, l'esprit d'équipe, la rigueur et le sens du devoir ont été des plus remarquables au cours de ces trois années. Je suis convaincu et fier de dire que le Centre est vraiment sous surveillance.

applique dans les faits ses politiques; et l'examen des activités de collecte de renseignements électromagnétiques particuliers menées en vertu d'autorisations ministérielles.

En outre, avant la fin de mon mandat en tant que commissaire, je présenterai au ministre un rapport sur l'examen que je mène actuellement à propos du partage par le Centre de renseignements électromagnétiques étrangers avec ses plus proches partenaires étrangers — la National Security Agency des États-Unis, le Government Communications Headquarters du Royaume-Uni, la Defence Signals Directorate de l'Australie ainsi que le Government Communications Security Bureau de la Nouvelle-Zélande. Le Centre et ses partenaires étrangers respectent leurs lois respectives en s'engageant à ne pas viser, dans leurs activités de collecte, les communications de citoyens d'un pays du « Five Eyes ». Il est d'ailleurs interdit au Centre de demander à un partenaire étranger d'entreprendre des activités que lui-même se voit interdire de mener en vertu de la loi. Toutefois, le partage d'information par le Centre avec ses partenaires étrangers pourrait avoir des répercussions sur un Canadien. Car c'est dans le partage international de renseignements personnels que le risque est le plus élevé plutôt que dans le partage entre partenaires du même pays. Mon rapport annuel de 2011-2012 renfermait une mise à jour de cet examen. Cette année, j'ai poursuivi mon examen en profondeur sur des questions de droit d'ordre général se rapportant à ce sujet et j'ai consulté à ce propos ma conseillère juridique indépendante.

D'autres examens prévus en 2013-2014 pourraient déborder sur l'exercice suivant, notamment l'examen des activités de protection des technologies de l'information du Centre menées en vertu d'autorisations ministérielles à l'appui des efforts du gouvernement du Canada pour contrer les cybermenaces; un examen de suivi des activités du Centre menées en vertu d'une directive ministérielle en vue d'identifier de nouvelles entités étrangères susceptibles de présenter un intérêt le renseignement étranger; et l'examen de suivi des efforts du Centre pour combler de nombreuses lacunes en rapport avec ses interactions avec les Forces armées canadiennes, qui ont été relevées par les évaluateurs internes du Centre. En outre, le Bureau envisage de poursuivre l'examen annuel 1) des autorisations ministérielles relatives aux renseignements

décrit les distinctions entre la sécurité nationale et la sécurité publique, le rôle et l'incidence de l'examen de même que l'intégration de la technologie et de la protection de la vie privée dans la sécurité nationale.

Au début du mois de mars, le directeur exécutif a prononcé une allocution dans le cadre d'un déjeuner-conférence lors de la 15e conférence annuelle organisée par le Centre d'études stratégiques et militaires de l'Université de Calgary sur le thème de la sécurité mondiale dans une perspective historique (*Global Security: Past, Present and Future*). Son discours, qui a porté sur le rôle de l'examen du renseignement, était axé sur quatre questions : Pourquoi l'examen est-il important? Dans quelle mesure peut-il être efficace et à quoi tient cette efficacité? Quel est le point de vue des agences de renseignement elles-mêmes concernant l'examen? Et quels sont les défis et l'avenir qui l'attendent?

PLAN DE TRAVAIL – EXAMENS EN COURS ET PRÉVUS

Dans le choix des examens, les commissaires adoptent une approche axée sur le risque. Un plan de travail étalé sur trois ans est mis à jour deux fois par an. L'élaboration du plan de travail s'appuie sur plusieurs sources. Deux sources importantes sont d'une part les séances d'information régulières du Centre sur les activités nouvelles et les changements qui touchent les activités en place, et d'autre part les rapports annuels classifiés que le chef du Centre présente au ministre de la Défense nationale sur les priorités du Centre et des problèmes d'importance relatifs à la loi, aux politiques et à la gestion.

Les résultats de plusieurs examens actuellement en cours devraient faire l'objet d'un rapport qui sera présenté au ministre de la Défense nationale au cours de l'année à venir et figurer dans le rapport annuel 2013-2014 de mon successeur. Parmi les sujets retenus pour ces examens, mentionnons les activités antiterroristes du Centre; un suivi à l'examen de cette année portant sur certaines activités de collecte de renseignements électromagnétiques étrangers; l'examen du cadre de validation et des mécanismes établis par le Centre pour vérifier qu'il

renseignements classifiés — qu'on ne peut divulguer dans le présent rapport public ni sur notre site Web — de sorte que le ministre puisse être parfaitement au courant de l'examen des activités du Centre par le commissaire. L'an dernier, des employés de mon bureau et moi-même avons également rencontré plusieurs universitaires et des professionnels intéressés par la surveillance des agences chargées de la sécurité et du renseignement pour discuter de mon rôle et de mon travail, et pour obtenir leur point de vue sur la manière d'assurer un examen encore plus efficace. En outre, mon bureau a fait des présentations devant cinq groupes de nouveaux employés du Centre qui assistaient à un cours d'apprentissage de base, obligatoire pour tous les nouveaux employés du Centre. Ces présentations donnent une idée de mon travail et du travail du Bureau, de la façon dont nous nous y prenons et de l'incidence de nos activités sur eux, en tant qu'employés du Centre.

Au cours de l'exercice écoulé, le Centre a présenté aux employés de mon bureau plusieurs séances d'information détaillées dans le cadre de la conduite des examens. Le Centre a également tenu une séance d'information condensée sur les changements et les problèmes importants d'ordre opérationnel, politique et organisationnel récents. J'ai assisté à une présentation interactive qui démontrait les capacités du Centre en matière de collecte de renseignements électromagnétiques étrangers, et comment il répond à un incident. L'exercice s'est révélé très efficace pour montrer comment les différentes unités du Centre, les nombreux employés et les nombreux ministères et organismes fédéraux coopèrent, en réponse à une priorité de premier plan du gouvernement du Canada. J'ai été frappé par la connaissance et le professionnalisme des employés du Centre et par leur dévouement manifeste à l'égard de leurs responsabilités respectives. En outre, mon équipe a assisté à la formation donnée par le Centre sur les activités de collecte de renseignements électromagnétiques étrangers ainsi que sur la sécurité des communications.

À la suite d'une conférence sur la sécurité et la vie privée tenue à l'Université de Montréal en octobre 2011, mon directeur exécutif a écrit un chapitre dans un ouvrage intitulé *Circulation internationale de l'information et sécurité,* publié à la fin de 2012. Ce chapitre s'inspirait de sa participation à l'un des groupes de réflexion de la Conférence et

PLAINTES CONCERNANT LES ACTIVITÉS DU CENTRE

En 2012-2013, mon bureau a été contacté par plusieurs personnes qui cherchaient à obtenir de l'information ou exprimaient des préoccupations concernant les activités du Centre. Toutefois, après évaluation des demandes de renseignements, il est apparu qu'elles ne relevaient pas du mandat du commissaire ou qu'elles manquaient de crédibilité. Aucune plainte concernant les activités du Centre ne justifiait une enquête menée par le commissaire. (Pour obtenir davantage d'information sur la procédure de plainte, consulter notre site Web.)

MANDAT SOUS LE RÉGIME DE LA *LOI SUR LA PROTECTION DE L'INFORMATION*

Je suis tenu, en vertu de la *Loi sur la protection de l'information*, de recevoir de l'information émanant de personnes astreintes au secret à perpétuité, qui ont l'intention de communiquer des renseignements opérationnels spéciaux — par exemple, certains renseignements se rapportant aux activités du Centre — en faisant valoir la primauté de l'intérêt public. Aucune affaire de ce genre ne m'a été signalée en 2012-2013. (Pour obtenir davantage d'information sur les responsabilités du commissaire vertu de la *Loi sur la protection de l'information,* consulter notre site Web.)

ACTIVITÉS DU BUREAU DU COMMISSAIRE

Dans le rapport annuel de l'an dernier, dans le but de dissiper les malentendus et de mieux informer le public concernant le Centre, mon mandat et mes activités, j'ai fourni plus de détails que jamais auparavant sur les activités du Centre, sur ce qu'examine le commissaire, sur la façon dont les examens sont menés et sur l'incidence des examens. Le travail suit son cours pour améliorer le site Web, qui renferme des renseignements détaillés sur les activités du Bureau. Naturellement, les commissaires fournissent au ministre de la Défense nationale d'autres

procédure l'aide également à évaluer la façon dont le Centre surveille et valide le fait que ces activités respectent ses politiques opérationnelles.

Constatations

J'ai passé en revue tous les incidents et les erreurs de procédure liés aux renseignements électromagnétiques étrangers et à la sécurité des technologies de l'information susceptibles de porter atteinte à la vie privée qui sont survenus en 2012, ainsi que les mesures subséquentes prises par le Centre pour rectifier le tir.

Il y avait un très petit nombre d'erreurs de procédure et j'ai été d'accord avec l'évaluation du Centre, selon laquelle ces erreurs étaient mineures et ne se traduisaient pas par des incidents portant atteinte à la vie privée.

D'après mon examen des dossiers du Centre et d'après la vérification indépendante faite par mon bureau des rapports figurant dans une base de données du Centre, je suis convaincu que ce dernier a pris des mesures correctives pertinentes en réponse au petit nombre d'incidents portant atteinte à la vie privée qu'il a consignés.

J'ai été particulièrement heureux de constater que certaines mesures correctives avaient été prises par le Centre pour éviter que des incidents du même genre ne se reproduisent. Par exemple, le Centre effectue désormais un examen mensuel de son dossier central pour s'assurer que toutes les activités correctives requises ont été menées à bien ou sont en cours. Le Centre a aussi rappelé à ses employés leur obligation de signaler immédiatement un incident. Il a établi une procédure de rappel à ses employés afin de s'assurer que certaines informations de ses systèmes sont à jour et conformes aux autorités en vigueur.

Conclusion

Mon examen des incidents relatifs à la vie privée et des erreurs de procédure consignés en 2012 par le Centre n'a donné lieu à aucune recommandation. Mon examen n'a pas révélé de lacunes ou de problèmes systémiques qui auraient exigé un suivi. Un examen anuel de ces incidents et de ces erreurs continuera d'être réalisé.

6. Examen annuel des incidents et des erreurs de procédure signalés par le Centre en 2012, qui ont touché ou auraient pu toucher la vie privée de Canadiens, et des mesures prises par le Centre pour régler le problème

Contexte

Le Centre tient un dossier central décrivant les incidents opérationnels internes qui ont ou auraient pu toucher la vie privée de Canadiens. Il y consigne tout incident qui risque de porter atteinte à la vie privée d'un Canadien d'une manière qui n'est pas prévue dans ses politiques opérationnelles ou qui va à l'encontre de ces politiques. La politique du Centre exige que les employés qui travaillent sur les renseignements électromagnétiques étrangers et sur la sécurité des technologies de l'information signalent et documentent les incidents relatifs à la vie privée de façon à montrer la conformité du Centre à ses obligations en vertu de la loi et à ses politiques, et à prévenir d'autres incidents. Il pourrait s'agir, par exemple, de l'inclusion par inadvertance d'information sur l'identité d'un Canadien dans un rapport du Centre ou le partage par erreur de certains rapports avec un destinataire qui n'était pas le destinataire visé.

Les examens horizontaux et approfondis des activités du Centre incluent un examen de tous les incidents relatifs à la vie privée et des erreurs de procédure se rapportant au sujet qui fait l'objet de l'examen et, le cas échéant, il en est fait mention dans les sommaires de ces examens. Mon équipe fait preuve de vigilance au cours des examens visant à relever ces types d'incidents, de sorte que nous puissions confirmer si le Centre les a également détectés et a pris les mesures voulues.

Cet examen annuel répond à plusieurs finalités, à savoir prendre connaissance des incidents et des erreurs de procédure survenus en 2012 ainsi que des mesures connexes; et donner de la matière pour élaborer le plan de travail du commissaire en lui indiquant s'il y a des problèmes systémiques ou des problèmes de conformité à la loi ou de protection de la vie privée des Canadiens qui devraient faire l'objet d'un examen de suivi. L'examen de ces incidents relatifs à la vie privée et des erreurs de

sont en place pour fournir des consignes suffisantes aux employés du Centre concernant la protection de la vie privée des Canadiens. Les employés connaissaient bien les politiques et procédures en question et ils ont agi en conformité avec celles-ci.

Par ailleurs, en 2012, en réponse à une recommandation formulée par le commissaire Cory dans son rapport de 2010, le Centre a commencé à utiliser un nouveau système sécurisé en ligne pour traiter les demandes et les divulgations de renseignements sur l'identité de Canadiens. Le Centre a fait à mes employés une démonstration du système qui est actuellement utilisé avec ses principaux clients et il a l'intention d'étendre son utilisation à d'autres partenaires dès le début de la prochaine année fiscale. D'après le Centre, le système a amélioré le délai de réponse et se traduit par un meilleur service aux clients. Il renforce la reddition de compte en améliorant le suivi et le repérage des demandes et des divulgations de renseignements sur l'identité des Canadiens et il renferme plusieurs caractéristiques propres à garantir la protection de la vie privée des Canadiens.

Conclusion

Aucune recommandation ne découle de mon examen. Le Centre a mené ses activités de divulgation de manière consciencieuse; toutes les demandes examinées étaient autorisées, justifiées et bien documentées.

S'il y avait un seul cas de non-conformité dans la divulgation par le Centre de renseignements concernant l'identité de Canadiens, les répercussions éventuelles sur la vie privée des Canadiens pourraient être importantes. C'est pourquoi les examens annuels d'un échantillon de renseignements divulgués se poursuivront. L'an prochain, mon bureau effectuera un examen détaillé de l'utilisation du nouveau système, de même que d'un échantillon des renseignements concernant l'identité de Canadiens divulgués aux partenaires internationaux du Centre.

5. Examen annuel d'un échantillon de renseignements concernant l'identité de Canadiens divulgués à des clients du gouvernement du Canada

Contexte

Des renseignements concernant l'identité de Canadiens peuvent être inclus dans les rapports du Centre portant sur des renseignements électromagnétiques étrangers si cette information est jugée essentielle à la compréhension ou à l'utilisation de ces renseignements. Cependant, toute information identifiant un Canadien doit être supprimée des rapports et remplacée par une mention générale du type « un Canadien ». Lorsqu'il reçoit ensuite une demande de précisions sur l'information supprimée, le Centre doit vérifier que le client dont elle émane dispose à la fois de l'autorisation et d'une justification opérationnelle pour obtenir ce genre de renseignements. Ce n'est qu'une fois satisfait que le Centre fournit l'information.

Mon équipe a choisi et examiné un échantillon d'environ 20 p. 100 du nombre total de renseignements divulgués par le Centre aux organismes ou aux ministères fédéraux au cours de la période allant d'octobre 2011 à juin 2012. L'échantillon comprenait des renseignements divulgués à tous les ministères et organismes qui avaient demandé des informations sur l'identité de Canadiens au cours de la période visée. Des employés de mon bureau ont examiné les demandes à l'appui des autorisations des clients ainsi que la justification présentée pour obtenir l'information sur l'identité de Canadiens, les rapports connexes du Centre concernant les renseignements électromagnétiques étrangers, ainsi que les renseignements effectivement divulgués sur l'identité de Canadiens.

Constatations

Il ressort de mon évaluation des renseignements examinés et des entretiens que le Centre a mené ses activités de divulgation en conformité avec la loi. Des politiques opérationnelles et des procédures

qu'elles aient été utilisées ou non dans ses rapports. J'ai constaté que pour les exercices 2010-2011 et 2011-2012, le Centre ne conservait que les communications privées essentielles pour les affaires internationales, la défense ou la sécurité, comme l'exige l'alinéa 273.65(2)*d*) de la *Loi sur la défense nationale*. Une fois encore cette année, la proportion de ces communications est demeurée très mince et le Centre a détruit la plupart d'entre elles. En outre, l'élaboration actuelle d'un nouvel outil qui aidera les analystes du Centre à identifier les communications interceptées qui pourraient être des communications privées constitue un pas dans la bonne direction. Le Bureau du commissaire examinera l'incidence de ce nouvel outil sur la conformité et la protection de la vie privée dans le cadre d'un examen ultérieur.

Dans le rapport de l'an dernier, j'ai indiqué que certains renseignements sur les communications interceptées impliquant des partenaires étrangers du Centre n'étaient pas aisément accessibles. Je trouve encourageant que, bien que les autorisations ministérielles ne l'exigent pas, le Centre ait reconnu l'importance de faire état de ces renseignements au ministre. Le Bureau du commissaire suivra de près l'évolution de cette question.

Il est également réconfortant de constater que, bien que ce ne soit pas une exigence d'une autorisation ministérielle particulière, le Centre a accepté de porter à la connaissance du ministre certains renseignements liés à la vie privée. Cette mesure pour protéger la vie privée des Canadiens aidera le ministre à mieux assumer ses responsabilités. Elle va d'ailleurs dans le sens d'une recommandation que j'avais formulée en 2010-2011 et qui était demeurée en suspens. Le ministre avait appuyé au départ le rejet de cette recommandation par le Centre; toutefois, après mûre réflexion, j'ai maintenu ma recommandation et j'en ai informé le ministre. Le Centre a reconsidéré la question, il est revenu sur sa décision de départ et il a prévenu le ministre qu'il mettrait en œuvre la recommandation.

Conclusion

Je n'ai formulé aucune recommandation.

4. d'examiner, en vue de vérifier leur conformité à la loi, un échantillon de mon choix de toute communication privée interceptée fortuitement par le Centre au cours de la conduite de ses activités sous le régime d'une autorisation ministérielle.

Communications privées

Le commissaire jauge le nombre de communications privées interceptées fortuitement et il vérifie la façon dont le Centre a traité et utilisé ces communications. Il est en mesure d'examiner toutes les communications privées que le Centre utilise et conserve.

Constatations

J'ai conclu que les activités menées en vertu des autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers pour 2010-2011 et 2011-2012 étaient autorisées.

En ce qui a trait à chacune des 11 activités de collecte de renseignements électromagnétiques étrangers, j'ai examiné certains renseignements clés se rapportant à l'interception et à la vie privée des Canadiens, ce qui me permettait de comparer les activités et de noter tout changement ou tendance d'importance au fil du temps. Je n'ai constaté aucun changement important touchant la portée ou le mode opératoire des activités qui nécessitait un examen approfondi de suivi d'activités particulières. Ces autorisations ministérielles ne renfermaient pas de changements importants par rapport à l'exercice antérieur et le Centre n'a pas apporté de changements importants aux technologies utilisées pour ces activités.

Les changements apportés par le Centre en 2010-2011 et 2011-2012 aux politiques opérationnelles applicables à ce type de collecte ont clarifié les autorités et les pratiques et renforcé la protection de la vie privée des Canadiens.

J'ai également examiné un échantillon de communications privées interceptées fortuitement que le Centre a reconnues et conservées,

4. Examen des autorisations ministérielles du Centre relatives à la collecte de renseignements électromagnétiques étrangers en 2010-2011 et 2011-2012

Contexte

Le paragraphe 273.65(8) de la *Loi sur la défense nationale* exige que le commissaire fasse enquête sur les activités du Centre exercées sous le régime d'une autorisation ministérielle « pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre [de la Défense nationale] ». Un examen combiné régulier des autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers constitue donc pour les commissaires une façon de s'acquitter de ce volet de leur mandat. Cet examen annuel couvre deux exercices : j'ai d'abord examiné les cinq autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers en vigueur du 1er décembre 2010 au 30 novembre 2011 qui se rapportaient à cinq activités ou catégories d'activités; j'ai ensuite examiné les six autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers en vigueur du 1er décembre 2011 au 30 novembre 2012 qui se rapportaient à six activités ou catégories d'activités. L'objet de mon examen était :

1. de m'assurer que les activités menées en vertu des autorisations ministérielles étaient autorisées et que le ministre était convaincu que les quatre conditions requises par les alinéas 273.65(2)*a*) à *d*) de la *Loi sur la défense nationale* avaient été respectées;

2. de signaler tout changement d'importance dans le texte même des autorisations ministérielles ou dans les activités du Centre décrites dans ces autorisations;

3. d'évaluer l'incidence, le cas échéant, de ces changements sur le risque de non-conformité et sur le risque d'atteinte à la vie privée et, en conséquence, de cerner tout sujet nécessitant un examen de suivi; et

Constatations

J'ai constaté que le Centre conduisait ses activités conformément à la loi et aux directives ministérielles, et aucune question ne s'est posée concernant les rapports et les renseignements conservés que j'ai passés en revue.

J'ai signalé que le Centre améliorerait sa capacité à montrer qu'il dispose de mesures pour protéger la vie privée des Canadiens en consignant le retour ou l'élimination de renseignenments non pertinents acquis par un propriétaire de système et partagés avec le Centre. Nonobstant cette suggestion, j'ai constaté que les activités à l'appui de la sécurité des technologies de l'information renfermaient des mesures satisfaisantes pour protéger la vie privée des Canadiens.

Au cours de la période visée par l'examen, des politiques opérationnelles et des procédures d'applications générales étaient en place pour fournir des lignes directrices générales concernant la conformité à la loi et la protection de la vie privée des Canadiens. Toutefois, il n'y avait pas de lignes directrices opérationnelles spécifiques régissant ces activités. Il est donc encourageant de voir que, après la période visée par l'examen, le Centre a émis une politique particulière pour la conduite de ces activités.

Quelques employés du Centre qui ont été interrogés ont été incapables de citer certaines politiques, mais ils étaient au courant des règles régissant leurs activités. De plus, les gestionnaires du Centre qui ont été interrogés surveillaient de près et de manière systématique les activités pour s'assurer que leurs employés se conformaient aux autorisations en vigueur. D'après les dossiers examinés, les réponses aux questions au cours des entretiens et les activités de validation de la conformité aux politiques du Centre, il ressort de mon examen que les politiques et les procédures pertinentes ont été respectées.

Conclusion

Mon rapport d'examen ne renferme pas de recommandations. Le Bureau continuera de mener sur une base régulière des examens approfondis des activités de protection des technologies de l'information non exécutées en vertu d'une autorisation ministérielle pour vérifier la conformité à la loi et dans quelle unesure le Centre protège la vie privée des Canadiens en menant les activités.

Les objectifs de mon examen étaient d'évaluer si le Centre s'est conformé à la loi et dans quelle mesure il a protégé la vie privée des Canadiens en exécutant ces activités. En plus d'acquérir une connaissance détaillée de ces activités, j'ai examiné :

- le cadre législatif et stratégique de ces activités;
- les changements organisationnels qui touchent le Centre;
- les technologies, les bases de données et les systèmes utilisés pour les activités;
- le volume et le traitement des communications privées et des renseignements sur l'identité de Canadiens acquis dans le cadre des activités, de même qu'un échantillon de ces communications privées et des renseignements sur l'identité de Canadiens utilisés par le Centre; et
- les accords en place avec les ministères et organismes fédéraux.

Communication privée : « communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine » (article 183 du *Code criminel*).

J'ai examiné les activités menées entre le 1er avril 2009 et le 31 mars 2011, et j'ai effectué un examen plus détaillé des activités et des rapports afférents pour un certain nombre de ministères et d'organismes aidés par le Centre au cours de cette période. En outre, les dossiers ont été passés en revue pour vérifier que les renseignements du propriétaire du système conservés par le Centre l'ont été en vertu d'une autorisation légale pertinente. Mon examen portait également sur les réponses du Centre à des aspects nécessitant un suivi et relevés dans une étude réalisée en 2009 par le commissaire Gonthier.

3. Examen des activités de protection des technologies de l'information non menées par le Centre en vertu d'une autorisation ministérielle

Contexte

La *Loi sur la défense nationale* stipule que le Centre a pour mandat de fournir des avis, des conseils et des services aux ministères et organismes du gouvernement du Canada, de même qu'à d'autres propriétaires de systèmes de technologies de l'information pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada (alinéa 273.64 (1)*b*)).

Au cours de la période visée par l'examen, le gouvernement du Canada a réorganisé ses efforts de cyberdéfense. Le Centre est devenu le premier point de contact pour les cyberincidents qui touchent les ministères et organismes fédéraux. Sécurité publique Canada est le principal point de contact pour les cyberincidents touchant les secteurs des infrastructures essentielles n'appartenant pas au gouvernement du Canada. Précisons par ailleurs que le Centre est responsable des cybermenaces d'une grande complexité, comme celles découlant d'agents d'État étrangers, tandis que Sécurité publique Canada prend en charge les menaces moins complexes, par exemple, celles se rapportant aux vulnérabilités connues des logiciels disponibles sur le marché.

J'ai examiné certaines activités menées par le Centre à l'appui de la sécurité des technologies de l'information pour détecter, analyser et atténuer les cybermenaces. Le Centre n'entreprend pas ces activités en vertu d'une autorisation ministérielle puisqu'il n'intercepte pas de communications. Il a plutôt recours dans ce cas aux renseignements acquis par les propriétaires de système — sous le régime d'autorisations en vertu du *Code criminel,* et par les propriétaires de systèmes du gouvernement du Canada, sous le régime, en plus, de leurs autorisations en vertu de la *Loi sur la gestion des finances publiques* — et divulgués au Centre. Ces autorités permettent l'interception de communications privées par des personnes autorisées lorsque cette interception est raisonnablement nécessaire pour protéger les systèmes informatiques des méfaits et d'une utilisation non autorisée.

droit de la vie privée. J'ai formulé deux recommandations à l'intention du ministre pour aider à faire en sorte que l'assistance donnée par le Centre au SCRS soit conforme aux autorités et respecte les limites des mandats, et pour renforcer les mesures en place en vue de protéger la vie privée des Canadiens. Plus précisément, je recommande que :

1. le Centre discute avec le SCRS l'application à d'autres situations d'une pratique existante pour protéger la vie privée; et

2. le Centre conseille au SCRS de fournir à la Cour fédérale du Canada certaines preuves supplémentaires quant à la nature et à l'ampleur de l'aide qu'il peut apporter au SCRS.

J'ai constaté que les pratiques du Centre liées à son aide au SCRS et les activités connexes étaient conformes aux exigences générales énoncées dans les directives ministérielles adressées au Centre concernant la « Vie privée des Canadiens » et le « Cadre de responsabilisation », à savoir qu'elles respectaient expressément la loi et qu'elles étaient assorties de mesures pour s'assurer que l'information était obtenue de manière légale et traitée en conformité avec la *Charte canadienne des droits et libertés* et la *Loi sur la protection des renseignements personnels*.

Conclusion

Même si j'ai formulé deux recommandations à l'intention du ministre pour assurer que l'aide apportée par le Centre au SCRS est conforme à la loi et pour renforcer la protection de la vie privée, ma conclusion est que le Centre a conduit ses activités en accord avec la loi et les directives ministérielles et d'une manière qui intègre des mesures pour protéger la vie privée des Canadiens. Le ministre a souscrit aux recommandations et le Centre y a donné suite.

Au terme de mon examen, j'ai envoyé au président du CSARS, à titre d'information, certaines observations générales se rapportant au SCRS, découlant des deux recommandations que j'avais formulées et que le CSARS voudra peut-être examiner au moment opportun. Le Centre m'a indiqué par la suite qu'il avait parlé des recommandations — qui se rapportent à des questions qui relèvent du SCRS ou exigent son aval — avec le SCRS.

Conclusions et recommandations

Au cours de la période visée par l'examen, le Centre a réagi de façon adéquate à deux incidents liés à la vie privée qu'il a relevés et qui concernaient la diffusion non intentionnelle de renseignements sur l'identité de Canadiens faisant l'objet de mandats. En fait, le Centre a déjà clarifié les processus internes pertinents pour la conduite de certaines activités et il a rappelé à ses employés leurs responsabilités à l'égard de la gestion de certains renseignements. Cela devrait aider à prévenir des incidents similaires.

J'ai interrogé le Centre concernant un autre incident ayant trait à l'interception de communications pour le compte du SCRS pendant quelques jours après l'expiration d'un mandat particulier. J'ai accepté les explications que m'a données le Centre concernant cet incident, selon lesquelles il s'agissait d'une erreur humaine non intentionnelle. Le Centre m'a également confirmé que les communications interceptées dans ce cas avaient été détruites et que le SCRS ne les avait pas reçues. Je suis convaincu que le Centre a répertorié cet incident et qu'il a rappelé à ses employés la procédure appropriée pour empêcher que des erreurs de ce genre ne se reproduisent.

Au cours de la période visée par l'examen, les politiques opérationnelles et les procédures applicables en général à l'aide apportée par le Centre à l'appui de ces mandats et à l'appui d'activités connexes étaient en place et ont fourni des consignes aux employés du Centre concernant la conformité à la loi et la protection de la vie privée des Canadiens. Après la période visée par l'examen, le Centre a émis des consignes précises pour la prestation de cette aide et la conduite des activités. De façon générale, les employés du Centre interrogés sont bien au courant des politiques et des procédures et ont montré qu'ils connaissaient leurs responsabilités respectives. Il ressort de mes entretiens avec les gestionnaires, les chefs d'équipe et les autres employés du Centre que les gestionnaires surveillent systématiquement l'aide et les activités connexes pour s'assurer qu'elles sont conformes aux autorités qui les requièrent.

Outre l'examen détaillé des activités du Centre en vertu des mandats, j'ai réfléchi à des questions générales de droit se rapportant à ce sujet et j'ai consulté ma conseillère juridique indépendante, qui est une experte en

renseignements par le SCRS avec l'assistance du CST[C], comme le propose le mandat, respecte le régime législatif approuvé par le législateur et ne contrevient pas à la *Charte* (*X (Re)* aux paragraphes 75-76).

Les objectifs de mon examen étaient de bien connaître et de documenter l'aide apportée par le Centre au SCRS et d'évaluer si les activités du Centre étaient conformes à la loi, y compris aux conditions des mandats délivrés au SCRS, et à toutes les protections de la vie privée qui étaient stipulées. L'assistance que le Centre porte au SCRS en vertu des mandats peut inclure de l'information sur l'identité d'un Canadien et l'interception de communications de Canadiens. La collecte du Centre, circonscrite par le mandat, peut avoir une incidence sur la vie privée de Canadiens.

Je me suis penché sur l'aide qu'a apportée le Centre au SCRS dans l'exécution d'un certain nombre des premiers mandats de ce genre émis en rapport avec la lutte antiterroriste. En particulier, dans le cadre de l'évaluation de la conformité à la loi et de la protection de la vie privée, en vertu des mandats examinés, j'ai vérifié que :

- le Centre avait copie du mandat et qu'il avait des renseignements clairs et suffisants concernant l'aide demandée par le SCRS;
- les communications ciblées par le Centre pour le SCRS étaient uniquement celles mentionnées dans les mandats;
- les communications n'avaient pas été ciblées avant l'entrée en vigueur des mandats et ont cessé de l'être à l'expiration des mandats;
- le Centre a ciblé les individus visés par les mandats uniquement lorsqu'ils étaient censés être à l'extérieur du pays;
- le Centre a ciblé uniquement les types de communications et d'information que les mandats l'autorisaient à intercepter ou à recueillir; et
- le Centre a respecté toutes les autres limites imposées par la loi au SCRS, par exemple toutes les conditions stipulées dans les mandats.

Canadiens en territoire étranger au moyen des capacités d'interception du Centre. La requête était étayée par la déclaration sous serment d'un employé du Centre qui décrivait les capacités d'interception de l'agence et la façon dont les communications seraient interceptées *depuis le Canada*.

L'alinéa 273.64(1)*c*) de la *Loi sur la défense nationale* autorise le Centre à fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère. En vertu de cette assistance, le Centre peut notamment appuyer le SCRS dans l'interception de communications de Canadiens si le SCRS dispose d'un mandat décerné par un juge en vertu de l'article 21 de la *Loi sur le Service canadien du renseignement de sécurité*. En vertu du paragraphe 273.64(3) de la *Loi sur la défense nationale*, le Centre doit respecter les limites que la loi impose à l'organisme auquel il donne assistance — par exemple, toutes les conditions imposées par un juge dans un mandat. Lorsque le Centre fournit une assistance opérationnelle au SCRS, il devient l'agent du SCRS. Le SCRS est *de jure* le propriétaire de l'information et des communications interceptées relatives à l'objet du mandat.

Dans *X (Re)*, le juge Mosley a déclaré :

> Le Canada a donné au CST[C] le mandat de collecter des renseignements étrangers, y compris des renseignements tirés de communications ainsi que de systèmes et de réseaux de technologie de l'information à l'étranger. La loi lui [CSTC] interdit de diriger ses activités contre des Canadiens ou contre toute personne se trouvant au Canada, mais elle ne l'empêche pas d'aider des organismes de sécurité et d'application de la loi agissant conformément à des délégations de pouvoir légales comme des mandats décernés par des tribunaux. Le SCRS a le pouvoir de collecter des renseignements concernant des menaces potentielles à propos de Canadiens et d'autres personnes et, comme il en a été question précédemment, il n'est pas assujetti à des limites territoriales.
>
> Lorsque les conditions préalables à la délivrance d'un mandat sont remplies, y compris le contrôle judiciaire préalable, les motifs raisonnables et des cibles bien précises, la collecte de

À ma demande, mon bureau a commencé à examiner d'autres activités de collecte de renseignements étrangers plus récentes, notamment le suivi des questions soulevées dans cet examen, et il s'emploiera à déterminer si les changements apportés aux politiques et aux procédures du Centre, depuis la période visée par l'examen, ont conduit à une amélioration de la clarté des échanges d'information entre le Centre et le SCRS.

Conclusion

Au 31 mars 2013, soit à la fin de la période visée par le rapport 2012-2013, j'attendais encore la réponse du ministre aux deux recommandations. Il sera fait état de ces réponses dans le rapport annuel du prochain exercice.

2. Aide du CSTC au SCRS en vertu de la partie *c*) du mandat du Centre et des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité*

Contexte

En 2007, le SCRS a demandé à la Cour fédérale du Canada un mandat l'autorisant à enquêter sur les activités d'individus en voyage à l'étranger susceptibles de constituer une menace. L'honorable juge Edmond Blanchard a soutenu que la Cour n'avait pas la compétence requise pour autoriser des activités d'enquête intrusives menées par le SCRS en territoire étranger (*Loi sur le Service canadien de sécurité (Re),* 2008 CF (301).

En 2009, dans *X (Re),* 2009 CF 1058, le SCRC a invité la Cour fédérale à réexaminer le raisonnement du juge Blanchard. Il demandait à la Cour de se pencher à nouveau sur la question de la compétence sur la base d'une description plus détaillée des activités requises pour effectuer l'interception et d'une argumentation juridique nouvelle qui expliquait en quoi la méthode même de l'interception est pertinente pour la détermination de la compétence de la Cour. L'honorable juge Richard Mosley s'est dit convaincu que les faits et le droit justifiaient que la demande soit considérée comme différente de celle dont avait été saisi le juge Blanchard et il a délivré le mandat autorisant le SCRS à intercepter les communications de

POINTS SAILLANTS DES SIX RAPPORTS D'EXAMEN PRÉSENTÉS AU MINISTRE EN 2012-2013

1. Examen de certaines activités de collecte de renseignements électromagnétiques étrangers

Contexte

J'ai examiné l'acquisition, l'utilisation et l'échange d'information par le Centre dans le cadre de certaines activités de collecte de renseignements électromagnétiques étrangers menées il y a quelques années.

Constatations et recommandations

La majorité des activités du Centre que j'ai examinées ne présentait aucun problème. Toutefois, un petit nombre de dossiers suggéraient la possibilité que des Canadiens aient été visés par certaines activités, ce qui est contraire à la loi. Certains dossiers du Centre relatifs à ces activités n'étaient pas clairs ou étaient incomplets. Après un examen minutieux et approfondi, je n'ai pas pu parvenir à une conclusion définitive sur la conformité ou non à la loi.

Au cours de l'examen, j'ai découvert qu'un certain nombre de dossiers du Centre se rapportant à des échanges d'information avec le SCRS manquaient parfois de clarté, ce qui m'a amené à recommander que le Centre adopte des lignes directrices concernant la façon de communiquer clairement et de manière cohérente avec ses partenaires à propos de l'entité visée. De même, j'ai recommandé que le Centre s'assure que ses analystes de renseignements étrangers soient au fait des lignes directrices existantes, adoptées depuis la période visée par l'examen, qu'ils sachent qu'il leur incombe de justifier leurs activités et de déterminer le statut étranger d'une entité visée, et qu'ils s'acquittent de leurs responsabilités. Au terme de mon examen, j'ai envoyé au président du CSARS, à titre d'information, certaines observations générales concernant le SCRS qui découlent des recommandations que j'ai formulées.

Deux examens menés cette année — l'examen de certaines activités de collecte de renseignements électromagnétiques étrangers et l'examen de l'aide du Centre au SCRS en vertu de la partie *c*) de son mandat et des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité* — ont relevé l'absence de certaines données historiques dans un système et une base de données du Centre se rapportant à la collecte de renseignements électromagnétiques étrangers. Ce système et cette base de données appuient le processus en vertu duquel le Centre détermine que des entités de renseignements électromagnétiques étrangers d'intérêt sont en fait bel et bien étrangères et situées à l'extérieur du Canada, comme l'exige la *Loi sur la défense nationale.* L'absence d'information a limité ma capacité à évaluer la légalité des activités du Centre à cet égard et pourrait également avoir une incidence sur l'examen d'autres activités du Centre. En raison de la gravité de cette situation, j'ai donné comme instruction à mon équipe de mener un examen approfondi de la question pour déterminer les implications et réfléchir à une solution. Cette question a prolongé le temps requis pour mener à bien les deux examens. Il est encourageant de voir que le Centre a déjà pris des mesures et continue à le faire pour assurer la disponibilité de l'information requise pour la reddition de compte et pour faire la preuve de sa conformité à la loi. Le Bureau du commissaire surveillera l'évolution de la situation.

Dans le rapport annuel de l'an dernier, j'ai exprimé ma frustration devant le fait que le Centre n'avait pas accordé à mon Bureau son soutien habituel et que certains examens avaient en conséquence subis des délais excessifs. Le Centre a pris des mesures pour corriger la situation et je suis convaincu que grâce à ces mesures l'année à venir sera productive.

Ces examens ont été réalisés en vertu de deux volets de mon mandat :

- m'assurer que les activités du Centre sont conformes à la loi — comme il est stipulé à l'alinéa 273.63(2)*a*) de la *Loi sur la défense nationale*; et
- m'assurer que les activités du Centre menées sous le régime d'une autorisation ministérielle sont conformes — comme l'établit le paragraphe 273.65(8) de la *Loi sur la défense nationale*.

Les résultats

Chaque année je présente un compte rendu général de mes constatations concernant la légalité des activités du Centre. À l'exception d'un examen décrit ci-dessous — dans le cadre duquel j'ai été incapable de parvenir à une conclusion définitive concernant la conformité ou non à la loi pour certaines activités de collecte de renseignements électromagnétiques étrangers — toutes les activités du Centre examinées cette année étaient conformes à la loi.

Par ailleurs, j'ai formulé quatre recommandations pour promouvoir la conformité à la loi et renforcer la protection de la vie privée. Les recommandations, qui sont décrites dans les résumés d'examen qui suivent, se rapportent au renforcement de l'orientation stratégique et à la généralisation d'une pratique existante de protection de la vie privée à d'autres situations, de même qu'à la communication à la Cour fédérale du Canada de certains éléments de preuve supplémentaires quant à la nature et à l'étendue de l'aide que le Centre peut offrir au SCRS.

En outre, j'ai envoyé à titre d'information au président du CSARS certaines observations générales concernant le SCRS, qui découlent des recommandations que j'ai formulées et que le CSARS voudra peut-être examiner en temps opportun. Cela montre bien la façon dont les organismes de surveillance en place peuvent, dans l'esprit des recommandations de la commission d'enquête dirigée par l'honorable juge Dennis O'Connor, collaborer en vertu de la législation actuelle dans la conduite d'examens des activités auxquelles participent plus d'une agence vouée à la sécurité ou au renseignement.

- a adopté une politique révisée d'aide opérationnelle aux organismes chargés de la sécurité et de l'application de la loi en vertu de la partie *c*) du mandat du Centre, y compris des lignes directrices sur la conservation et l'élimination des dossiers liés à cette aide;
- a adopté une procédure révisée définissant le risque et l'atténuation du risque pour certaines activités de collecte de renseignements électromagnétiques étrangers, de même que l'adoption d'un cadre de gestion du risque pour la planification et l'approbation de ces activités; et
- a lancé un nouveau système sécurisé de concert avec d'autres ministères et organismes fédéraux pour le traitement et le suivi des demandes et des divulgations de renseignements supprimés sur l'identité de Canadiens.

Ces mesures prises par le Centre montrent bien que l'examen porte fruit. Le Bureau du commissaire examinera l'incidence de ces améliorations sur la conformité et la protection de la vie privée dans ses examens ultérieurs. En outre, le Bureau du commissaire surveille six recommandations auxquelles le Centre donne suite actuellement. Les réponses du ministre à deux des recommandations de cette année ne nous étaient pas encore parvenues au moment de la rédaction du présent rapport.

Vous trouverez sur notre site Web une liste complète des 74 rapports d'examen classifiés présentés au ministre de la Défense nationale.

APERÇU DES CONSTATATIONS ET RECOMMANDATIONS DE 2012-2013

Au cours de l'exercice 2012-2013 visé par le rapport, j'ai présenté au ministre de la Défense nationale six rapports portant sur mes examens des activités du Centre.

du Centre, qui a connu une croissance importante. Je suis épaulé dans mon travail par un effectif de huit personnes, auxquelles s'ajoutent plusieurs experts-conseils recrutés au fil des besoins. En 2012-2013, les dépenses du Bureau se sont élevées à 2 285 718 $, ce qui ne dépasse pas les limites du budget global approuvé par le Parlement.

L'**annexe C** présente l'état des dépenses du Bureau du commissaire du Centre de la sécurité des télécommunications pour 2012-2013 (p. 47).

IMPACT DES RECOMMANDATIONS DU COMMISSAIRE

Depuis 1997, mes prédécesseurs et moi-même avons présenté au ministre de la Défense nationale 74 rapports d'examen classifiés. Au total, ces rapports renfermaient 138 recommandations. Le Centre a souscrit à 92 p. 100 (127 sur 138) de ces recommandations et il a pris ou prend actuellement des mesures pour y donner suite.

Les commissaires surveillent la façon dont le Centre donne suite à ces recommandations et répond aux constatations négatives de même qu'aux aspects nécessitant un suivi mentionnés dans les examens antérieurs. Au cours de l'année écoulée, le Centre m'a avisé qu'il a mis en œuvre intégralement 14 recommandations antérieures. Entre autres, le Centre :

- a aidé le ministre de la Défense nationale à mettre à jour certaines directives ministérielles;
- a mis à jour les protocoles d'entente généraux pour l'échange d'information et la coopération opérationnelle avec le SCRS et le ministère des Affaires étrangères et du Commerce international;
- s'est engagé à communiquer au ministre de la Défense nationale certains renseignements (que l'on ne peut mentionner pour des raisons de sécurité) en vue de protéger la vie privée des Canadiens et d'appuyer le ministre dans sa reddition de compte en sa qualité de responsable du Centre;

Indépendance

Bien que je présente mes rapports au ministre de la Défense nationale responsable du Centre, le Bureau du commissaire est complètement indépendant et bénéficie de son propre crédit parlementaire. Mon mandat est étayé par les pouvoirs dont je suis investi en vertu de la *Loi sur les enquêtes,* notamment le pouvoir d'assigner à comparaître, qui me garantissent l'accès à toute information et aux employés du Centre.

Commissaire du Centre

Le commissaire occupe une charge indépendante créée par la loi et ne reçoit pas d'orientation générale du premier ministre, du ministre de la Défense nationale ou de tout autre ministre sur la façon de s'acquitter de son mandat. Le commissaire permet au gouvernement du Canada de garder le Centre sous contrôle en fournissant des avis au ministre à l'appui de son processus décisionnel et de son obligation redditionnelle à l'égard du Centre. Les rapports classifiés du commissaire adressés au ministre, et le rapport annuel non classifié adressé au Parlement et au public par l'intermédiaire du ministre, indiquent si le Centre a agi en conformité avec la loi et la mesure dans laquelle il a protégé la vie privée des Canadiens dans la conduite de ses activités.

L'annexe B renferme le texte des articles pertinents de la *Loi sur la défense nationale* et de la *Loi sur la protection de l'information* se rapportant à mon rôle et à mon mandat en tant que commissaire du Centre (p. 43). (Pour obtenir davantage d'information sur l'histoire du Bureau du commissaire du Centre de la sécurité des télécommunications, consulter notre site Web.)

BUREAU DU COMMISSAIRE

L'an dernier, les travaux d'agrandissement des locaux du Bureau ont pris fin et l'on dispose de suffisamment de place pour les fonctions actuelles, ainsi que pour les responsabilités additionnelles résultant de l'autonomie budgétaire du Bureau. L'agrandissement me permettra d'embaucher deux agents supplémentaires afin de pouvoir mener un examen adéquat

- utilise, partage, communique, conserve ou détruit les renseignements interceptés; ou
- prend des mesures pour protéger les communications privées interceptées fortuitement ainsi que l'information concernant des Canadiens.

Conduite d'enquêtes

En vertu de mon mandat, je suis tenu d'entreprendre toute enquête que je juge nécessaire à la suite d'une plainte formulée par écrit — par exemple pour déterminer si le Centre a mené ou mène une activité non conforme à la loi ou s'il ne prend pas suffisamment de mesures pour protéger la vie privée des Canadiens. (Pour obtenir davantage d'information sur les responsabilités du commissaire dans la conduite des enquêtes sur les plaintes, consulter notre site Web.)

Informer le ministre

En vertu de mon mandat, qui consiste à informer le ministre de la Défense nationale :

- je fais état des résultats de mes examens dans des rapports classifiés adressés au ministre; et
- je présente chaque année un rapport non classifié sur mes activités au ministre, lequel doit ensuite le déposer au Parlement. Il s'agit ici du 17e rapport annuel.

Si je suis tenu avant tout de faire état des incidents de non-conformité du Centre, je dois également, en vertu de mon mandat, informer le ministre de toute activité qui, à mon avis, pourrait présenter un risque de non-conformité, notamment l'interception illégale d'une communication privée ou toute autre atteinte à la vie privée d'un Canadien. Plusieurs de mes rapports incluent des recommandations axées sur la prévention, car l'un des buts du Bureau du commissaire est de renforcer les pratiques du Centre qui favorisent la conformité et intègrent des mesures propres à protéger la vie privée des Canadiens.

Politiques et procédures : Je m'attends à ce que le Centre dispose de politiques et de procédures pertinentes pour orienter ses activités et donner des consignes suffisantes sur les obligations légales et les exigences ministérielles, notamment en matière de protection de la vie privée des Canadiens. Je m'attends à ce que les employés soient au courant des politiques et procédures et qu'ils s'y conforment. Je m'attends aussi à ce que le Centre dispose de mécanismes efficaces de validation de la conformité et assure le maintien de l'intégrité de ses opérations. Le Centre doit être en mesure de rendre compte de façon adéquate des décisions importantes prises et de justifier l'information liée à la conformité et à la protection de la vie privée des Canadiens.

Mes rapports d'examen classifiés décrivent les activités et les pratiques du Centre et font état de constatations relativement aux critères susmentionnés. Ces rapports peuvent également indiquer la nature et l'importance des dérogations observées par rapport à ces critères. Dans certains cas, je formule des recommandations à l'intention du ministre, qui visent à corriger les écarts entre les activités du Centre et les attentes suscitées par les critères d'examen.

Le modèle logique de l'**annexe A** présente un organigramme de notre programme d'examen (p. XX).

Examens horizontaux

Les examens horizontaux portent sur les processus communs à l'ensemble des méthodes de collecte de renseignements électromagnétiques étrangers du Centre ou des activités de protection des technologies de l'information. Mentionnons, par exemple, les processus en vertu desquels le Centre :

- identifie et choisit les entités étrangères d'intérêt pour le renseignement situées à l'extérieur du Canada ou représentant une menace pour les systèmes informatiques du gouvernement du Canada, et dirige ses activités vers elles;

Information sur les Canadiens : tout renseignement personnel (au sens de la *Loi sur la protection des renseignements personnels*) à propos d'un Canadien, y compris une personne morale canadienne.

Méthode et critères d'examen

Mes examens des activités sont *ex post*, c'est-à-dire qu'ils portent sur des activités qui ont été menées dans le passé. Toutefois, ils incluent toujours un examen des raisons *ex ante* qui expliquent pourquoi le Centre mène ces activités — afin de confirmer que les justifications des activités du Centre sont légitimes et ressortent de son mandat. Lorsqu'il procède à un examen, mon bureau passe en revue les dossiers sur papier et électroniques du Centre, de même que ses politiques et procédures ainsi que les avis juridiques reçus du ministère de la Justice Canada. Mon équipe requiert la tenue de séances d'information et de démonstrations portant sur des activités particulières, interroge des gestionnaires et des employés du Centre et observe par elle-même les opérateurs et les analystes lorsqu'ils sont à l'œuvre pour vérifier la façon dont ils effectuent leur travail. Mon équipe vérifie l'exactitude de l'information recueillie en la comparant au contenu des systèmes et des bases de données du Centre.

Chaque examen comporte une évaluation des activités du Centre selon une série de critères standard, décrits ci-après, relatifs aux obligations légales, aux exigences ministérielles et aux politiques et procédures du Centre. Chaque examen peut comporter des critères supplémentaires selon les besoins.

Obligations légales : Je m'attends à ce que le Centre mène ses activités en conformité avec la *Loi sur la défense nationale*, la *Charte canadienne des droits et libertés*, la *Loi sur la protection des renseignements personnels*, le *Code criminel* et toute autre législation pertinente, et en conformité avec les avis du ministère de la Justice Canada.

Exigences ministérielles : Je m'attends à ce que le Centre mène ses activités en accord avec les instructions ministérielles, c'est-à-dire conformément à toutes les exigences ou limites précisées dans une autorisation ou une directive ministérielle.

gouvernement du Canada de tout méfait ou de toute utilisation non autorisée ou de toute perturbation de leur fonctionnement. Dans chaque cas, la loi précise les conditions en vertu desquelles une autorisation ministérielle peut être émise. Les autorisations ministérielles se rapportent à une activité ou à une catégorie d'activités précisées dans l'autorisation — c'est-à-dire qu'elles visent expressément une méthode d'acquisition de renseignements électromagnétiques étrangers ou de protection des systèmes informatiques (le comment); toutefois, les autorisations ne se rapportent pas à une personne ou à un sujet en particulier (le qui ou le quoi). La loi exige également que le commissaire du Centre examine les activités menées en vertu d'une autorisation ministérielle et qu'il rende compte chaque année de cet examen au ministre de la Défense nationale. (Pour obtenir davantage d'information sur les autorisations ministérielles de même que sur les pouvoirs et les limites applicables aux activités du Centre, consulter notre site Web.)

Sélection des activités visées par l'examen

Pour arrêter mon programme d'examen, j'adopte une approche préventive et axée sur le risque. Je choisis de préférence les activités du Centre où le risque de non-conformité à la loi est le plus élevé, notamment au chapitre du respect de la vie privée des Canadiens, en tenant compte de divers facteurs :

- les contrôles exercés par le Centre sur l'activité pour assurer la conformité aux obligations légales, aux exigences ministérielles et aux politiques du Centre (les autorités);
- la question de savoir si l'activité peut mettre en jeu des communications privées ou de l'information concernant des Canadiens;
- le fait que l'activité soit nouvelle, qu'elle ait subi d'importants changements ou qu'il se soit écoulé beaucoup de temps depuis un dernier examen en profondeur;
- la possibilité que d'importants changements aient été apportés aux exigences ou aux technologies se rapportant à l'activité;
- la nécessité d'un suivi établie par les commissaires dans un rapport antérieur; et
- les enjeux soulevés dans le domaine public.

Examen des activités du Centre

Mon mandat consiste à examiner les activités du Centre qui se rapportent à la collecte de renseignements électromagnétiques étrangers, à la protection des renseignements électroniques et des infrastructures d'information d'importance du gouvernement du Canada et à l'aide fournie aux organismes fédéraux chargés de l'application de la loi et de la sécurité.

L'objet de mon mandat en matière d'examen consiste :

- à déterminer si les activités que mène le Centre en vertu d'une autorisation ministérielle sont bien celles autorisées par le ministre de la Défense nationale, et à vérifier que les conditions d'autorisation requises par la *Loi sur la défense nationale* sont remplies;
- à déterminer si le Centre se conforme à la loi et, si je pense qu'il pourrait ne pas avoir agi en conformité avec la loi, en aviser le ministre de la Défense nationale et le procureur général du Canada;
- à vérifier que le Centre, dans ses activités de collecte de renseignements électromagnétiques étrangers et de protection des technologies de l'information, ne vise pas des Canadiens; et
- à promouvoir l'élaboration et l'application efficaces de mesures satisfaisantes pour protéger la vie privée des Canadiens dans toutes les activités que le Centre entreprend.

Protection des Canadiens

Le Centre se voit interdire par la loi, dans le cadre de ses activités de collecte de renseignements électromagnétiques étrangers ou de protection des technologies de l'information, de viser des Canadiens — où qu'ils se trouvent dans le monde — ou toute personne au Canada.

Autorisations ministérielles

La *Loi sur la défense nationale* habilite le ministre de la Défense nationale à autoriser par écrit le Centre à intercepter fortuitement des communications privées alors qu'il recueille des renseignements électromagnétiques étrangers ou protège les systèmes informatiques du

MANDAT DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

Le mandat dont j'ai été investi en vertu de la *Loi sur la défense nationale* comprend trois grandes fonctions :

1. **procéder à des examens concernant les activités du Centre** pour en contrôler la légalité;

2. **faire les enquêtes** que j'estime nécessaires à la suite de plaintes concernant le Centre; et

3. **informer le ministre** de la Défense nationale, qui est responsable du Centre devant le Parlement, et le procureur général du Canada de toutes les activités du Centre qui, à mon avis, pourraient ne pas être conformes à la loi.

J'ai en outre pour mandat, en vertu de la *Loi sur la protection de l'information,* de recevoir de l'information émanant de personnes astreintes au secret à perpétuité qui souhaitent communiquer des renseignements opérationnels spéciaux du Centre en faisant valoir la primauté de l'intérêt public. (Pour obtenir davantage d'information sur les responsabilités du commissaire au titre de la primauté de l'intérêt public, consulter notre site Web.)

Mandat du Centre

Lorsque la *Loi antiterroriste* est entrée en vigueur le 24 décembre 2001, elle a ajouté la partie V.1 à la *Loi sur la défense nationale* et établi le mandat à trois volets du Centre :

- la partie *a*) autorise le Centre à acquérir et à utiliser des renseignements électromagnétiques étrangers en conformité avec les priorités du gouvernement du Canada en matière de renseignement;
- la partie *b*) autorise le Centre à aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada; et
- la partie *c*) autorise le Centre à fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, notamment pour qu'ils obtiennent et déchiffrent les communications recueillies en vertu de leurs autorités respectives.

modifications qui élimineraient les ambigüités signalées par mes prédécesseurs et moi-même, je l'ai dit à plusieurs reprises, auraient pour effet de bonifier des dispositions adoptées à toute vapeur dans la foulée des attentats du 11 septembre 2001. À mon avis, elles ne devraient pas soulever de controverse.

L'indépendance du Bureau du commissaire

Le Bureau a obtenu son indépendance institutionnelle et financière il y a un peu plus de cinq ans quand il s'est vu confier son propre budget approuvé par le Parlement. Jusqu'alors, son budget faisait partie de celui du ministère de la Défense nationale. Pour souligner cette indépendance, le commissaire a émis pour la première fois, en 2011, son premier communiqué faisant état du dépôt au Parlement de son rapport annuel par le ministre de la Défense nationale. L'autonomie financière a cependant ses revers. Le Bureau, qui est un petit organisme disposant d'un budget d'environ 2 millions de dollars, est astreint aux mêmes exigences en matière de comptabilité que les autres ministères dont le budget se chiffre parfois en termes de milliards de dollars. C'est là, me semble-t-il, un cas de bureaucratie excessive qui se traduit par la préparation d'une foule de rapports dont l'utilité est douteuse aussi bien pour mon bureau que pour ceux qui s'y intéressent.

Sur un plan bilatéral, mon bureau s'est employé à tisser des liens dès que l'occasion se présentait avec des interlocuteurs étrangers. L'an dernier, par exemple, j'ai rencontré les membres d'une délégation de parlementaires français en quête d'information sur la nature et le fonctionnement des agences canadiennes de surveillance. J'ai aussi eu des discussions avec des membres du Comité permanent de contrôle des services de renseignements et de sécurité de la Belgique. À un autre moment, j'ai rencontré les membres du comité parlementaire britannique du renseignement et de la sécurité. Je souhaite que ce genre de rencontres se répète plus souvent.

La cybersécurité et les cyberattaques

On ne peut plus parler de sécurité sans évoquer les cybermenaces. Il ne se passe pas de semaine où le risque de pénétration de systèmes informatiques publics et privés ne fait pas la manchette. Le Centre, de par son mandat, est appelé à jouer un rôle déterminant dans la protection des renseignements électroniques et des infrastructures d'information importantes pour le gouvernement du Canada. C'est Sécurité publique Canada qui veille, de son côté, à la protection des infrastructures essentielles qui peut impliquer le secteur privé, tirant profit au besoin de l'expérience du Centre.

Comme il est inévitable qu'au cours de certaines activités de protection des technologies de l'information, le Centre soit amené à intercepter fortuitement des communications privées de Canadiens, mon bureau a fait preuve ces dernières années d'une vigilance accrue dans ce domaine. Des examens ont été menés à bien, d'autres sont en cours et je suis convaincu que mon successeur maintiendra le cap à cet égard.

Les modifications législatives à la *Loi sur la défense nationale*

J'avais entrepris mon mandat avec la conviction que les modifications à la *Loi sur la défense nationale* proposées par mes prédécesseurs seraient adoptées sous peu. Elles ne l'ont pas encore été. J'avoue être profondément déçu du manque d'empressement du gouvernement, lequel n'a plus aujourd'hui l'excuse d'un statut minoritaire. Ces

Une autre forme de collaboration entre les organismes de surveillance est apparue récemment. Mon bureau offre un séminaire d'apprentissage aux nouveaux employés des différentes agences de surveillance. L'objectif est d'expliquer diverses méthodes de surveillance et de contribuer au développement de pratiques d'examen plus rigoureuses.

Le partage des renseignements avec des partenaires étrangers

Avec l'accroissement de la collaboration internationale dans ce domaine, il est important de s'assurer que les pays et organismes étrangers avec lesquels le Canada échange des renseignements protègent avec autant de rigueur que nous la vie privée des Canadiens lorsque la situation se présente. Ce n'est pas là une tâche facile. D'une part, en effet, les nations sont souveraines et ne souffrent guère d'interventions dans leurs affaires internes, surtout en matière de sécurité. D'autre part, les organismes et mécanismes de surveillance varient d'un pays à un autre. En l'absence de normes internationales, le meilleur moyen de protéger la vie privée des Canadiens dans le partage de renseignements avec les partenaires étrangers est de travailler à l'établissement dans les autres pays d'organismes de surveillance qui soient forts et indépendants, ce que nous faisons déjà dans une certaine mesure.

Depuis un quinzaine d'années, tous les deux ans, une conférence regroupe les agences de surveillance d'une douzaine de pays, dont les membres du groupe dit des « Five Eyes » (Canada, États-Unis, Grande-Bretagne, Australie et Nouvelle-Zélande). Cette rencontre ouvre des perspectives nouvelles et est source d'échanges enrichissants et de découvertes stimulantes. Qui plus est, ces conférences permettent à des pays où le principe d'une surveillance indépendante émerge à peine, de participer comme observateurs et de s'inspirer de ce qui se passe ailleurs. Le Canada a été l'hôte de cette conférence en mai 2012.

C'est dans ce contexte que mon bureau organise à l'occasion des déjeuners-rencontres avec des spécialistes des domaines de la sécurité nationale et de la protection de la vie privée. Ces derniers tirent grand profit à mieux connaître nos méthodes de travail, et nous tirons grand profit à mieux connaître leurs points de vue et leurs intérêts.

La complémentarité des activités des agences canadiennes de surveillance

Mon bureau et le Comité de surveillance des activités de renseignement de sécurité (le CSARS) ont des fonctions similaires, mais nous sommes régis par des lois différentes qui ne nous donnent pas l'autorité voulue pour conjuguer nos efforts. Le Centre et le SCRS opèrent également en vertu de lois différentes, mais leurs lois respectives les autorisent à collaborer. Tandis que le Centre et le SCRS collaborent et mènent des actions conjointes, mon bureau et le CSARS n'ont pas la possibilité de mener une enquête conjointe. Il existe quand même une certaine possibilité de collaboration en vertu de la législation actuelle. Ainsi, par exemple, dans les domaines où je n'ai pas le mandat pour faire le suivi, je peux renvoyer au CSARS certaines questions pertinentes concernant le SCRS. Outre ce type d'activités, une collaboration formelle, comme le partage des renseignements opérationnels spéciaux, pourrait requérir l'intervention et l'approbation du cabinet et peut-être des modifications législatives. L'idéal serait que les lois permettent, voire encouragent d'office une telle collaboration.

La création d'une superstructure proposée dans le rapport d'une commission d'enquête antérieure, laquelle regrouperait les agences de surveillance, ne me paraît pas une solution utile à ce stade. Avant de créer une superbureaucratie additionnelle, avec la lourdeur et les coûts que cela entraîne, il me semble plus sage d'essayer d'utiliser au maximum les organismes déjà en place et de leur permettre d'unir leurs efforts quand la situation l'exige.

Le maintien de saines relations avec le Centre

Il me paraît indispensable qu'un organisme sous surveillance, à savoir le Centre, et qu'une agence de surveillance, mon bureau, cultivent des relations fondées sur le respect et la confiance. Le Centre a, de par la loi, l'obligation de prendre des mesures pour protéger la vie privée de toute personne au Canada et des Canadiens où qu'ils soient dans le monde. Le commissaire, de par la loi, a le mandat de s'assurer que le Centre se conforme à cette obligation. La protection de la vie privée est donc un objectif que le Centre et mon bureau ont en commun. Aussi m'apparaît-il essentiel que la relation de surveillance n'en soit pas une de supériorité, mais de complémentarité. Avec le recul, je vois mon bureau davantage comme la conscience du Centre que comme une épée de Damoclès, et je crois que le Centre me perçoit de plus en plus ainsi.

Je suis en mesure d'affirmer que les chefs en poste, John Adams d'abord, John Forster ensuite, n'ont ménagé aucun effort pour développer au sein du Centre une culture de respect de la loi et de la vie privée des Canadiens. Tous deux ont été des interlocuteurs honnêtes, coriaces parfois, mais toujours de bonne foi.

La transparence

Dès mon entrée en fonction, je me suis affairé à démystifier, sous réserve bien sûr des contraintes inévitables imposées par la sécurité nationale et par la sécurité publique, ce culte du secret qui imprègne les activités des services du renseignement ou de sécurité. Je crois que j'ai réussi dans une certaine mesure à vulgariser les termes on ne peut plus rébarbatifs utilisés dans ce milieu. Le plus beau compliment qu'on m'ait fait est celui d'avoir, dans mes rapports annuels, décrit mes activités et celles du Centre avec un degré de précision jusque-là inédit. Il reste beaucoup à faire, encore, mais je crois que la glace est brisée et que les autorités concernées comprennent mieux aujourd'hui qu'il est possible, sans trahir des secrets d'État et sans mettre en péril la sécurité nationale, d'expliquer avec beaucoup plus d'ouverture le travail qu'elles font. Plus la transparence sera grande, plus le scepticisme et le cynisme de la population iront s'atténuant.

MESSAGE DU COMMISSAIRE : UN COURT BILAN AU TERME DE MON MANDAT

Au moment où le ministre de la Défense nationale déposera ce rapport annuel devant le Parlement, je viendrai tout juste de compléter mon mandat de trois ans à titre de commissaire du Centre de la sécurité des télécommunications (le Centre ou CSTC). Je viendrai tout juste, aussi, et ce, pour des raisons personnelles, de décliner l'offre de renouvellement de mon mandat. On me permettra de faire un court bilan de mon passage à la tête du Bureau du commissaire.

Les rapports et recommandations

Au cours de mon mandat, j'ai présenté au ministre de la Défense nationale 19 rapports d'examen. Ces rapports couvraient à peu près tous les aspects des activités du Centre, y compris celles menées en vertu d'autorisations ministérielles ou à la demande d'organismes voués à la sécurité ou à l'application de la loi. J'ai donc examiné toute une panoplie d'activités, entre autres : la collecte de renseignements électromagnétiques étrangers, la protection des renseignements électroniques et des infrastructures d'information importantes pour le gouvernement du Canada, et l'assistance technique et opérationnelle apportée par le Centre, notamment au Service canadien du renseignement de sécurité (SCRS). Mes rapports comprenaient 12 recommandations.

L'intégrité du processus d'examen et la crédibilité du Bureau du commissaire dépendent en grande partie du suivi effectué par le Bureau de la mise en œuvre par le Centre de ces recommandations. Je suis heureux de souligner que depuis 1997, 127 des 138 recommandations (soit 92 p. 100) contenues dans les 74 rapports classifiés que les commissaires ont remis au ministre ont été acceptées et mises en œuvre ou sont en voie de l`être. En d'autres termes, les mécanismes de protection de la vie privée qui sont en place sont constamment bonifiés et adaptés aux réalités mouvantes de la technologie et des opérations. À l'occasion, des recommandations ont entraîné la suspension par le Centre de certaines de ses activités pour réexaminer comment elles sont mises en œuvre, de même que des changements importants dans les politiques et pratiques adoptées par le Centre.

BIOGRAPHIE DE L'HONORABLE ROBERT DÉCARY, C.R.

L'honorable Robert Décary, c.r., a été nommé commissaire du Centre de la sécurité des télécommunications le 18 juin 2010 pour un mandat de trois ans.

Né à Montréal en 1944, le commissaire Décary a fait ses études au Collège Jean-de-Brébeuf (B. A.), à l'Université de Montréal (LL.L.) et à l'Université de Londres (LL.M.). Il est devenu membre du Barreau du Québec en 1967 et a reçu, en 1986, le titre de conseiller de la reine.

Au cours de sa carrière consacrée à la chose publique, au droit et au journalisme, il a notamment été adjoint spécial auprès de l'honorable Mitchell Sharp, alors secrétaire d'État aux Affaires extérieures du Canada (1970–1973), co-directeur de la recherche à la Commission de l'unité canadienne (la Commission Pepin-Robarts) (1978–1979), et membre du Comité de rédaction constitutionnelle française du ministère fédéral de la Justice (1985–1990).

Il a pratiqué le droit à Montréal, puis à Gatineau, où il s'est spécialisé, au sein du cabinet Noël, Décary, dans la représentation de nombreux cabinets d'avocats et du procureur général du Québec auprès de la Cour suprême du Canada.

Il a écrit de nombreuses chroniques dans *Le Devoir* et *La Presse* et il a contribué à plusieurs revues et ouvrages juridiques. Il est l'auteur d'un *Aide-mémoire sur la Cour suprême du Canada* (1988) et de *Chère Élize (ou la grande et la petite histoire du rapatriement)* (1983).

Il a été membre de la Cour d'appel fédérale de 1990 à 2009. En 2009, il était nommé arbitre du Tribunal arbitral du sport (Lausanne, Suisse) et en 2010, il devenait membre du Centre de règlement des différends sportifs du Canada.

Plaintes concernant les activités du Centre /36

Mandat sous le régime de la *Loi sur la protection de l'information* /36

Activités du Bureau du commissaire /36

Plan de travail — Examens en cours et prévus /38

En guise de conclusion /40

Annexe A : Programme d'examen du Bureau du commissaire — Modèle logique /41

Annexe B : Extraits de la *Loi sur la défense nationale* et de la *Loi sur la protection de l'information* relatifs au mandat du commissaire /43

Annexe C : État des dépenses de 2012–2013 /46

TABLE DES MATIÈRES

Biographie de l'honorable Robert Décary, c.r. /2

Message du commissaire : Un court bilan au terme de mon mandat /3

Mandat du commissaire du Centre de la sécurité des télécommunications /9

Bureau du commissaire /15

Impact des recommandations du commissaire /16

Aperçu des constatations et recommandations de 2012–2013 /17

Points saillants des six rapports d'examen présentés au ministre en 2012–2013 /20

1. Examen de certaines activités de collecte de renseignements électromagnétiques étrangers /20

2. Aide du CSTC au SCRS en vertu de la partie *c*) du mandat du CSTC et des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité* /21

3. Examen des activités de protection des technologies de l'information non menées par le Centre en vertu d'une autorisation ministérielle /26

4. Examen des autorisations ministérielles du Centre relatives à la collecte de renseignements électromagnétiques étrangers en 2010–2011 et 2011–2012 /29

5. Examen annuel d'un échantillon de renseignements concernant l'identité de Canadiens divulgués à des clients du gouvernement du Canada /32

6. Examen annuel des incidents et des erreurs de procédure signalés par le Centre en 2012, qui ont touché ou auraient pu toucher la vie privée de Canadiens, et des mesures prises par le Centre pour régler le problème /34

3269

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Robert Décary, c.r.

CANADA

Communications Security
Establishment Commissioner

The Honourable Robert Décary, Q.C.

Juin 2013

Ministre de la Défense nationale
Édifice MGén G.R. Pearkes, 13e étage
101, promenade Colonel By, tour Nord
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63(3) de la *Loi sur la défense nationale*, j'ai l'honneur de vous transmettre le rapport annuel faisant état de mes activités et constatations pour la période allant du 1er avril 2012 au 31 mars 2013, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Le commissaire,

Robert Décary

P.O. Box/C.P. 1984, Station "B"/Succursale « B »
Ottawa, Canada
K1P 5R5
Tél. : 613-992-3044 Téléc. : 613- 992-4096

Bureau du commissaire
du Centre de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : 613-992-3044
Téléc. : 613-992-4096
Site Web : www.ocsec-bccst.gc.ca

© Ministre des Travaux publics et des
Services gouvernementaux Canada 2013
N° de catalogue D95-2013
ISSN 1206-7490

Graphisme de couverture : Cameron Fraser

FSC
www.fsc.org
MIXTE
Papier issu
de sources
responsables
FSC® C103458



COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

RAPPORT ANNUEL 2012-2013

Canada